

From: [David Andrejcek](#)  
To: (b) (6); [Andrew Dodge](#); (b) (6)  
Subject: FW: September 13 news clips  
Date: Thursday, September 13, 2018 9:24:11 AM

---

See the Lake Worth story below.

---

From: (b) (6) On Behalf Of MediaDL  
Sent: Thursday, September 13, 2018 9:14 AM  
To: NewsDL <NewsDL@ferc.gov>  
Subject: September 13 news clips



Thursday, September 13, 2018

Visit our [News Clips](#) website

## **TOP STORIES. 2**

[FERC, NERC to probe power outages during winter cold snap. 2](#)

[FERC, NERC investigate winter outages. 3](#)

[FERC chairman: Steps to speed up LNG project reviews will be good for industry. 4](#)

## **ELECTRIC. 5**

[PJM continues trying to untangle subsidized resources from its capacity market 5](#)

[Did gunman open fire on Lake Worth transformer, blacking out city?. 6](#)

## **GAS/LNG/OIL PIPELINES. 11**

[Court tosses class-action suit over New England gas, power activity. 11](#)

[Libertarian group goes to bat over pipelines, property rights. 13](#)

[Environmentalists press US FWS to dig deeper on species surveys for Atlantic Coast Pipeline. 14](#)

[Delaware River Basin Commission asks FERC for say on pipeline work in watershed. 16](#)

[FERC urged to block tree-cutting before final decisions on PennEast pipeline. 17](#)

[Pennsylvania landowners cite inactivity in asking FERC to rescind Constitution Pipeline permit 19](#)

## **CONGRESS. 21**

[Senate approves energy and water bill 21](#)

## **STATES. 22**

[Worst-case scenario plans in place as Florence bears down. 22](#)

[Duke Energy 'ready to attack' Florence, forecasts up to 3 million outages. 25](#)

[US STORM: Utilities expect massive outages, high repair costs from Florence. 27](#)  
[Hurricane Florence expected to dampen gas demand in US Southeast 29](#)  
[Carolinas race to bolster fragile dams. 31](#)  
[Pa. lawmakers call for Mariner East work halt after blast on other ETP pipe. 33](#)  
[SCE proposes \\$582 million plan to prevent grid-related wildfires. 34](#)

## Top Stories

S&P Global Platts  
 September 12, 2018

### FERC, NERC to probe power outages during winter cold snap

By Molly Christian, S&P Global Market Intelligence

The US Federal Energy Regulatory Commission and North American Electric Reliability Corp. have launched a joint inquiry into power outages and other grid issues that occurred in the Midwest and part of the South Central US during a mid-January cold snap, FERC announced Wednesday.

The probe comes as the Trump administration considers policies to support economically challenged coal -fired and nuclear power plants that the US Department of Energy said were crucial in meeting higher electricity demand during extremely cold weather this past winter.

That weather pattern caused the southern portion of the Midcontinent ISO 's footprint to experience a record winter peak of 32.1 GW on January 17, according to a quarterly report from Potomac Economics, which serves as MISO 's independent market monitor. Voluntary load curtailments helped reduce demand, but forced outages still rose to nearly 7.5 GW by early January 17. The tough conditions prompted MISO to declare an emergency during the evening peak on January 17 and early the following day.

FERC said the joint study will seek to identify the causes of multiple forced outages, voltage deviations and "near-overloads" that took place in the regions at issue during the week of Jan. 15. But the probe is not an enforcement investigation, the commission added.

"Inquiries of this type are ... among the many steps that we take to protect and safeguard the reliability of the bulk power system," FERC Chairman Kevin McIntyre said in a related news release. NERC President and CEO Jim Robb said the review could provide beneficial lessons for the industry ahead of the upcoming winter season.

FERC and NERC staff will work on the inquiry with the Midwest Reliability Organization , Reliability First Corp., SERC Reliability Corp and relevant companies.

#### DOE actions

The probe follows the DOE 's March release of a controversial study warning that further retirements of coal -fired and nuclear units, which have struggled to compete against growing gas -fueled generation, could threaten grid reliability and resilience during severe weather events. The DOE report came out days before merchant generator FirstEnergy Solutions asked the agency to issue an emergency order that would require the PJM Interconnection to buy power, capacity and other services from certain coal and nuclear plants in the region at risk of closure.

The DOE has yet to decide on FirstEnergy Solutions' request, but a draft plan leaked in late May would require regional grid operators to purchase power or capacity for two years from

certain "fuel-secure" power plants to bolster national defense. Critics of the DOE efforts say such actions would disadvantage gas-fired and renewable energy and distort competitive power markets.

FERC spokesperson Craig Cano said he could not provide additional information on FERC's inquiry with NERC, including on how the study could inform future policy changes. The commission in January asked grid operators to identify their resilience concerns after rejecting a prior DOE push to protect vulnerable coal and nuclear plants, but FERC has yet to propose new rules or other policies in response to the review.

[Return to Top](#)

E&E newsPM

September 12, 2018

GRID

## FERC, NERC investigate winter outages

[Sam Mintz](#), E&E News reporter

Federal energy regulators announced today that they are investigating outages that plagued the electric grid during an extreme cold weather event in January.

The Federal Energy Regulatory Commission and North American Electric Reliability Corp. launched a joint inquiry to examine issues on the grid in the midwestern and south-central United States on Jan. 17, when grid operators reported forced generation outages, voltage deviations and near-overloads.

The effort is not an enforcement investigation, but it will focus on identifying causes of the event and come up with recommendations to improve operations for the next time such conditions occur.

"Inquiries of this type are ... among the many steps that we take to protect and safeguard the reliability of the bulk power system," FERC Chairman Kevin McIntyre said in a statement.

NERC President Jim Robb said the inquiry is "timely" because it will help identify lessons to be learned ahead of this coming winter.

"It is also especially relevant that as the Western Interconnection Reliability Coordinator function fragments among multiple providers that we understand and underscore the importance of seamless RC-to-RC interactions," he said in a statement.

Peak Reliability, the reliability coordinator for most of the Western Interconnection, is shutting down at the end of next year, and multiple entities are planning to fill the gap, including the Southwest Power Pool and California Independent System Operator.

The grids on the East Coast and in the Midwest successfully weathered extreme cold earlier in January, while both sides of an ongoing debate about the best way to ensure resilience used statistics from the "bomb cyclone" to bolster their arguments ([Energywire](#), Jan. 4).

Twitter: [@samjmintz](#) Email: [smintz@eenews.net](mailto:smintz@eenews.net)

[Return to Top](#)

S&P Global

September 11, 2018

## FERC chairman: Steps to speed up LNG project reviews will be good for industry

By Corey Paul

Federal Energy Regulatory Commission Chairman Kevin McIntyre said recent steps to speed up reviews of U.S. natural gas liquefaction and export projects will make things easier for developers.

"Our recent streamlining efforts will provide all LNG stakeholders additional regulatory certainty and help minimize undue administrative burdens," McIntyre said in a Sept. 11 podcast produced by the commission. "These process improvements have shortened projected environmental schedules in some cases by 9 to 12 months. [The improvements] will help to ensure that FERC will be equipped to process applications in a timely and expedient manner without compromising its statutory obligation to ensure safety and environmental protection."

FERC on Aug. 31 issued 12 new and updated environmental schedules for LNG projects, at a time when the commission faced pressure to address a backlog of applications for the export facilities.

The notices of environmental schedules came with the announcement that FERC had agreed to work with the Pipeline and Hazardous Materials Safety Administration, part of the U.S. Department of Transportation, to improve coordination between the two agencies on siting and safety reviews. FERC is the lead federal agency in preparing environmental assessments and impact statements under the National Environmental Policy Act for LNG and natural gas infrastructure projects.

Other steps FERC took to process LNG applications more quickly included hiring new staff focused on LNG, using an outside contractor to help with construction inspections, and working with project developers to hire third-party contractors to conduct analyses that involve nonproprietary information.

While several market watchers joined developers in describing the recent FERC actions as favorable to the U.S. LNG export industry, some observers said there were limits to the benefits.

"While positive in the sense that FERC is attempting to streamline the liquefaction project approval process, our understanding is that the major regulatory bottleneck at this time is engineering reviews (not environmental)," Barclays analysts wrote in a Sept. 10 note to clients. "Until more clarity is provided with respect to reducing engineering review timelines, there does not appear to be any expectation for an accelerated FERC approval process (yet)."

McIntyre also used the podcast to reiterate support for FERC Chief of Staff Anthony Pugliese, who has made public comments that prompted questions over the agency's impartiality from a member of a U.S. Senate oversight committee.

Asked during the in-house podcast if Pugliese is "speaking for you," McIntyre said, "The Federal Energy Regulatory Commission speaks through its orders, not through speeches, tweets or other statements of the commission's chairman, other commissioners or staff, although those too are avenues of communication that we use under appropriate circumstances without them purporting to serve as statements of commission policy."

Pugliese had criticized Democrats in an interview with the conservative Breitbart News for an anti-energy infrastructure stance and accused them of playing politics. Separate comments by

Pugliese in a speech to a nuclear industry group had stoked concerns among Democratic lawmakers that the commission's independence was at risk.

McIntyre praised Pugliese, saying he played a key role in boosting coordination with other federal entities, including the recent agreement with PHMSA.

"He is highly qualified to serve as chief of staff because of his demonstrated leadership ability," McIntyre said.

[Return to Top](#)

## Electric

S&P Global Platts  
September 12, 2018

### PJM continues trying to untangle subsidized resources from its capacity market

By Jared Anderson

As PJM Interconnection prepares to file tariff revisions with federal regulators regarding changes to its capacity market structure designed to address subsidized resources, stakeholders Tuesday discussed PJM's plan, along with how to handle New Jersey's recently enacted nuclear subsidy law.

The US Federal Energy Regulatory Commission on June 29 rejected two proposals from PJM designed to mitigate the effects of state-subsidized energy resources on the region's capacity market. FERC established a proceeding (EL18-178) to work out details of the plan, which PJM and its stakeholders discussed at Tuesday's Markets & Reliability Committee special session on the issue.

The grid operator has been refining its definition of "subsidy," which it currently characterizes as a material subsidy received "in any way" by a capacity marketseller for a capacity resource that is greater than 1% of that resource's "actual or reasonably anticipated" total revenues from markets administered by PJM, according to the tracking document being used to formulate the FERC filing.

PJM's updated proposal will only consider subsidies that the capacity market seller is "entitled to" at the time the election for a resource carve-out is due. A capacity market seller with an annual resource, which is subject to the minimum offer price rule because it is receiving a subsidy, is eligible to elect a carve-out for that resource.

Market participants that choose to elect a resource carve-out must do so 120 days prior to the start of the base residual auction, which has been pushed back to August from May next year to allow ample time for these rule changes to be approved and implemented.

PJM noted that if a resource receives an actionable subsidy after the BRA, the MOPR will be applied in the incremental auctions for that delivery year and the resource will not be eligible for a carve-out as the load will already have been included in the BRA for that delivery year.

#### New Jersey ZECs

Some stakeholders asked how the "eligible" subsidy distinction would be handled in the case of New Jersey where legislation was recently passed to allow nuclear power plant owners to apply for zero-emissions credits.

The state's legislature passed the ZEC law in April, and it was signed by Governor Phil

Murphy, a Democrat, in May. Under the legislation, the New Jersey Board of Public Utilities is to pursue contracts with nuclear generators for credits for no more than 40% of the state's retail electric deliveries. The board would have 330 days from the date of enactment to select which generators would receive payments for three years.

PJM's executive director of market operations, Adam Keech, said there was a "little bit of a complexity there," and clarified that PJM would not consider New Jersey nuclear resources "eligible" to receive subsidies until the BPU had approved their ZEC requests.

"We expect to begin receiving payments at the end of the first quarter of 2019," Chris Crane, Exelon's CEO, told analysts May 2 during a conference call to discuss first-quarter financial results.

Exelon subsidiary, Exelon Generation, owns a 43% share of the two-unit 2,486-MW Salem nuclear plant in Salem County, New Jersey, which gives the company access to nuclear capacity that is potentially eligible to receive ZECs. PSEG Nuclear owns the majority share of Salem and also owns the adjacent 1,240-MW Hope Creek nuclear plant.

[Return to Top](#)

**Palm Beach Post**

September 13, 2018

## Did gunman open fire on Lake Worth transformer, blacking out city?

By [Joe Capozzi](#) - Palm Beach Post Staff Writer

---

LAKE WORTH —

It was disturbing enough that a transformer in the city's main electrical substation exploded in a fireball on a calm April night, [knocking out power](#) for seven hours to all of Lake Worth.

But after the fire was out, crews inspecting the damaged device saw something sinister — a jagged hole that looked like it was intentionally made by a projectile, perhaps even a bullet. They also noticed holes and nicks in other nearby equipment.

Did a gunman try to sabotage the city's electrical grid? Could the outage have been domestic terrorism?

Or was the culprit something all too familiar to long-term residents — faulty equipment?

Knowing that gunmen had attacked electrical equipment in California and Arkansas in recent years, city utility officials said the unusual circumstances around the explosion gave them no choice but to consider foul play.

"I don't want people to think that somebody is out there attacking us," said Ed Liberty, the city's director of electric utility. "But we have to be open to the evidence and not rule it out because we have this obligation to try to understand, as best as possible, what happened."

The FBI was called. The Palm Beach County Sheriff's Office opened an investigation. The damaged transformer was sent to a forensic lab for analysis.

Then, it happened again.

On the night of June 20, another fireball lit the sky over the same substation: A second transformer had catastrophically failed, causing a [citywide power outage](#) for nearly seven hours.

No suspicious holes were found on the second damaged device, which was directly next to the



one that failed April 9. But that offered city officials little comfort.

More than two months later, they still don't know why two transformers, which both passed technical tests when they were installed next to each other in March, failed without warning within a span of nearly three months.

Although PBSO investigators don't suspect foul play, city officials say they can't rule out an intentional act until the forensic investigations of both damaged transformers are completed later this year.

"There's too much evidence leaning both ways," said Walt Gill, assistant director. "Until the final report comes out, I'm not going to hang my hat either way."

## **'They are sitting ducks'**

If it was foul play, it wouldn't have been the first time someone intentionally tampered with the city's electric utility.

Last year, someone with an imaginative mind hacked into a database of pre-written public alerts, which are automatically posted online when the power goes out. During Hurricane Irma, an alert blaming an outage on "extreme zombie activity" was caught by city officials before it posted online.

But eight months later, the same zombie alert somehow made it online long enough during a 30-minute outage in May for residents to see it. It went viral, resulting in international headlines and lots of laughs.

The city still doesn't know who was responsible, but the zombie alerts seemed like a fitting metaphor for the utility's troubled past. For decades, Lake Worth has struggled with problems on its power grid — from sporadic outages to aging equipment, all generating sharp criticism from residents fed up with high rates and spotty service.

Utility officials say they are making strides to improve service. But because of that troubled history, they can understand if some longtime residents might have been skeptical when [sabotage was first mentioned](#) at a public meeting in July as a possible cause of the April 9 outage.

But the other troubling reality is that attacks on power stations in North America are not unheard of. Many are the result of vandals making mischief or bored hunters taking pot shots at tantalizing targets on utility poles, incidents that rarely make headlines.

Others, though, have been more serious.

In April 2013, a gunman with a precision assault rifle fired [more than 100 shots](#) at an [electrical substation in San Jose](#), Calif., causing millions of dollars in damage to 17 giant transformers that feed power to Silicon Valley. Officials at Pacific Gas & Electric avoided a blackout by rerouting power around its Metcalf substation, but it took 27 days to bring the station back to life. No arrests were made.

Although the FBI ruled out terrorism, Jon Wellinghoff, who was chairman of the Federal Energy Regulatory Commission at the time, disagreed and called the Metcalf attack "the most significant incident of [domestic terrorism](#) involving the grid that has ever occurred."

That same year, transformers and power stations in rural [Arkansas were targeted](#) in three consecutive attacks that led to the arrest of [a local man](#) who the FBI said acted alone. And in October 2013, members of a drug cartel used guns and Molotov cocktails to attack 18 power stations in Mexico, knocking out power for 420,000 people for 15 hours.

Those attacks highlighted what utility executives and federal energy officials have worried about for years — that the [electric grid is vulnerable to sabotage](#), said Tom Carlton of Illinois-based Infrastructure Defense Technologies.

From large transmission towers to power lines attached to poles, most electrical equipment sits out in the open, often in remote locations, protected only by chain-link fences.

“They are what we in the homeland security defense business call ‘soft targets’ because they are unprotected by security personnel,” said Carlton, whose firm specializes in perimeter security.

“They are sitting ducks, every one of them, for the most part.”

## Installed in March

The two transformers that exploded at Lake Worth’s Hypoluxo substation were inside a large rectangular area surrounded on three sides by 20-foot cinder-block walls and on the north side by a 6-foot chain-link fence topped with barbed wire.

The substation is often referred to as the city’s “tie-in line” because it’s the only location where city power lines tie in with the Florida Power & Light transmission system that winds throughout the state like an interstate highway network. It functions as an off-ramp from FPL’s main lines, distributing 138,000 volts through a local network of transformers to the city’s main plant and, ultimately, to 27,000 customers in the city.

The transformers that exploded in April and June are connected to the substation, but they are used only to measure the amount of electricity, or electrical current, coming in from FPL. Technically called “current transformers,” they’re casually referred to in the industry as CTs.

Each is about 8 feet high with a skinny ribbed porcelain body topped by a square tank covered by a protective weather dome, bearing an abstract resemblance to a robot.

The ones that exploded were made in 1995 by GEC Alsthom. They had been used for years at other locations in the city without incident before being moved into storage, Liberty said. He did not know when or why they were taken out of service.

They were re-installed at the Hypoluxo substation in March along with a third CT, each mounted next to the other atop 10-foot-high steel pedestals.

All three passed mandatory technical tests before they were put back into service, said Liberty. And the two that experienced sudden catastrophic failures showed no signs of an impending problem, he said.

## Did someone fire a shot?

At 11:14 p.m. on April 9, one of the three CTs exploded, plunging the city into darkness. Minutes later, utility crews from the city and FPL arrived at the Hypoluxo substation and saw flames leaping from the top of the transformer.

When the device cooled down to allow a safe inspection, a crew member in a lift bucket discovered a large hole on the side of the protective dome atop the transformer. The hole faced north toward a tree line visible through the chain-link fence.

“Inside that bowl you see this thing that looks like a softball-size chunk and that lined up with the hole on the side,” Liberty said. “It looked like somebody took a shot at it. It looked like a projectile had gone through it.”

They also noticed two small dents on a copper pipe, 25 feet above the ground, that supplied



power to the transformer. And on the chain-link fence, they saw bullet holes on metal informational signs, holes that lined up with the damaged transformer.

“Your first reaction is to look around and make sure no one out there is aiming a gun at you. You’re hoping whoever did it is not around,” recalled Michael Jenkins, the city’s energy delivery manager, describing the reaction of many of the 20 utility crewmen on site that night when gunman suspicions were first raised.

The next day, Jason Bailey, senior system operator for Lake Worth, called the sheriff’s office and reported that the transformer looked like it “had been tampered with.” Deputies notified the FBI, following protocol with suspicious incidents to public utility equipment, but the agency held off on getting involved and told PBSO to investigate, Liberty said.

The large hole on the side of the transformer’s dome “raised the suspicion that the transformer may have been purposely targeted and shot at with an unknown firearm,” according to [a PBSO report](#).

On April 12, detectives inspected the substation. From the ground, they noted that the dents on the copper pipe “appear to have similar indentations consistent with a metal projectile striking another metal object.” Citing danger from the high voltage lines, deputies said they could not look closer to confirm whether or not the dents were made by bullets.

Deputies canvassed the substation and the surrounding field for shell casings but couldn’t find any. They also spoke to the residents of three nearby homes. None reported hearing gunshots, but they did recall hearing “a loud boom” and seeing the transformer on fire.

A search for shell casings in the neighborhood came up empty. And PBSO records showed no calls about gunfire in the area that week.

## **No evidence of a crime**

Deputies also went to the city’s utility yard on Second Avenue North, where the damaged transformer had been taken earlier that day. They found no indications of damage from an outside projectile. The edges of the hole in the protective dome were “peeled outwards indicating an extreme pressure build up internally from an explosion,” the report said, contradicting the initial assessment by utility workers.

“On one side of the housing there is a large hole not consistent with an impact from a bullet. I could not find any fragments inside the housing, which would be components of a bullet such as copper jacketing or pieces of a lead core,” an investigator wrote.

Liberty said he doesn’t dispute PBSO’s report, but he said he and other utility officials thought parts of the hole looked like they peeled inward.

Bailey told deputies he still thought the damage to the CT “appeared suspicious.” He explained that when a transformer fails, monitors at the utility’s operations center would have shown a steady drop in power prior to the failure. In this case, he said, the power flow had been normal until the moment the device exploded.

The report makes no mention of the bullet holes on the metal information signs attached to the chain-link fence, but Liberty concedes that those holes might’ve been there before the CT failed.

PBSO filed the case as “an information report until further evidence is presented that a crime was committed.”

The city sent the damaged transformer to a lab at George Tech University, called the National

Electric Energy Testing, Research and Applications Center, for forensic analyses.

The final report, which will cost the city at least \$18,000, is expected later this year. But a preliminary draft doesn't mention an outside projectile as a cause and instead points to an internal failure with the device.

Oil samples from the transformer, taken by the city, showed moisture that had somehow breached the device. That moisture may have caused insulation material inside the CT to deteriorate, generating combustible gases, according to a draft summary of the preliminary report.

But city officials say there's no way to know when or how the moisture got into the oil. It could have come from rain that fell on the damaged CT after the explosion but before the transformer was removed from its pedestal. And while the moisture might have gotten in before the explosion, as the NEETRAC draft summary indicates, city officials say they saw no signs of leakage on the device when it was tested and installed.

Before NEETRAC finished its preliminary report on the April 9 incident, the second transformer exploded. City officials saw no suspicious marks on that device, but they are sending it to Georgia Tech for analysis, too. That second CT also had signs of moisture breach, according to oil samples taken by the city.

The city's third CT was taken off line as a precaution. The city has ordered four new ones at a cost of \$50,000. Until they are installed later this year, FPL has agreed to temporarily take over the role of measuring the amount of current the city takes from the substation, Liberty said.

Later this year, the city will replace the chain-link fence on the north side of the substation with another concrete block wall, meaning the entire substation will be protected in a roofless tomb 20-feet high.

City officials hope the final report rules out sabotage, which the preliminary report did not do.

"You're trying to walk a fine line and not panic the population," Liberty said. "But no data told us ahead of time that the device was about to fail and suddenly it fails. And we have evidence suggesting an outside cause.

"We don't know what it is, but it's certainly not something that should have happened."

[Return to Top](#)

## Gas/LNG/Oil Pipelines

S&P Global Platts  
September 12, 2018

### Court tosses class-action suit over New England gas, power activity

By Kate Winston

The US District Court for the District of Massachusetts has dismissed a class-action lawsuit alleging New England gas pipeline activity by Avangrid and Eversource Energy resulted in \$3.6 billion in overcharges for power, finding in part that the court should not wade into federal ratemaking for wholesale power.

The court concluded Tuesday that the suit's requested damages and injunctive relief run afoul

of the so-called filed rate doctrine, which says that rates approved by a federal agency such as the US Federal Energy Regulatory Commission must prevail over other claims seeking different rates.

“Federal and state antitrust claims, as well as state tort actions, that require courts to set aside or second guess rates approved by FERC must fail as a matter of law,” the court said.

In November, a batch of 12 New England electricity consumers filed a class-action lawsuit (Breiding et al. v. Eversource Energy et al., 1:17-cv-12274) against Avangrid and Eversource, which are local distribution companies in the region.

#### Withholding allegations

The suit alleged that Avangrid and Eversource used their no-notice contracts on Algonquin Gas Transmission to cancel capacity at the last minute without penalty, effectively shrinking the gas pipe and preventing others from using the capacity. The plaintiffs alleged this activity artificially inflated wholesale gas prices, which increased wholesale and retail electricity prices in New England. The suit alleged the activity aimed to boost prices paid to non-gas -fired plants, including hydro, wind and solar facilities owned by the defendants.

The lawsuit cited a study funded by the Environmental Defense Fund that found New England power customers paid on average 20% more for electricity than they would have in 2013-2016 because of gas pipeline capacity withholding by Avangrid and Eversource Energy. But FERC staff in February found that the study was flawed and led to incorrect conclusions about the alleged activity. Commission staff said it found no evidence of capacity withholding and would not take further action.

New England is increasingly relying on gas -fired generation, said Kieran Kemmerer, a power sector analyst with S&P Global Platts Analytics. “Gas -fired generation in ISO New England YTD (Jan – Aug) has increased 4% from the same period in 2017, and has averaged 48% of generation market share,” he said. “For reference nuclear generation has the next largest generation market share YTD, averaging 31% of total generation.”

#### Lawsuit dismissed

The court on Tuesday concluded the filed rate doctrine prevents the court from second-guessing FERC’s regulation of ISO-NE wholesale power rates, as well as FERC’s approval of no-notice pipeline contracts.

“To award monetary relief to retail electricity consumers, the court would be required to determine the difference between wholesale electricity rates during the class period and hypothetical rates that would have been charged but for defendants’ purported anticompetitive conduct,” the court noted. “This is exactly the analysis the filed rate doctrine prohibits.”

Avangrid said the court correctly determined that the filed rate doctrine bars the claims and that the plaintiffs lack standing, among a variety of other deficiencies. “We hope that the Court’s opinion and FERC Enforcement’s press release send a message to minimize frivolous claims that seek to disparage the hard work that our utilities are doing to provide safe and reliable service to our customers,” Scott Mahoney, Avangrid’s general counsel, said Wednesday.

Eversource spokesman Al Lara said the company was pleased the court quickly dismissed the case, noting the suit was based on an “erroneous” report sponsored by EDF.

[Return to Top](#)

EnergyWire  
September 13, 2018  
LAW

## Libertarian group goes to bat over pipelines, property rights

[Ellen M. Gilmer](#), E&E News reporter

A right-leaning think tank is again wading into the debate over landowner rights and oil and gas pipelines.

The Niskanen Center filed an amicus brief Tuesday urging the U.S. Court of Appeals for the District of Columbia Circuit to side with opponents to the Mountain Valley pipeline, a natural gas project that stretches across West Virginia and Virginia.

Niskanen's brief argues that the Federal Energy Regulatory Commission's approval process for gas pipelines routinely violates landowners' constitutional rights.

"No court has ever held that property owners can be forced to wait indefinitely for the constitutionally-required hearing on the taking of their land, and this Court should not be the first," the brief said.

At issue is FERC's rehearing process. Under the Natural Gas Act, pipeline builders can use the power of eminent domain to take property for pipeline construction as soon as they receive a certificate from FERC. Any challenges to FERC's certificate go through a rehearing process that often stretches out for months or even a year.

Project opponents generally cannot go to court to challenge a certificate until that rehearing process concludes. But extensive pipeline construction typically moves forward in the meantime ([Energywire](#), Sept. 13, 2017).

Niskanen's brief notes that the Supreme Court has repeatedly ruled that property owners are entitled to a hearing before or, in some cases, promptly after property is taken.

"The due process issue in this case arises because the hearing that results in a taking is held before an administrative agency that cannot adjudicate the property owners' constitutional claims, but the agency then indefinitely delays a judicial hearing of those claims," Niskanen attorney David Bookbinder wrote.

Bookbinder, formerly chief climate counsel for the Sierra Club, told E&E News the libertarian Niskanen Center is taking up the cause because "the odds are stacked against landowners."

"There are real serious legal questions here as to whether or not pipelines are a 'public use' such that they are entitled to eminent domain," he said.

Niskanen is working on the pipeline issue in a variety of venues.

The group also filed an amicus brief in state-level litigation in Iowa over the use of eminent domain for the Dakota Access oil pipeline. That case was argued yesterday in the Iowa Supreme Court.

In October, it is bringing on a new staff attorney to focus on pipelines and property rights. Niskanen plans to increase its friend-of-the-court filings and will begin representing landowners in pipeline-related litigation.

To date, the think tank has represented plaintiffs in only one case: a lawsuit from Colorado

municipalities seeking to hold oil and gas companies accountable for their products' contribution to climate change.

Niskanen has also been looking for allies on Capitol Hill. The group held a briefing with other property rights advocates last week to explain landowner concerns to Hill staffers and others.

The think tank also hired a lobbyist this year to shop around a bill that would reform parts of FERC's process ([Energywire](#), Feb. 14).

Twitter: [@ellengilmer](#) Email: [egilmer@eenews.net](mailto:egilmer@eenews.net)

[Return to Top](#)

**S&P Global Platts**  
September 12, 2018

## **Environmentalists press US FWS to dig deeper on species surveys for Atlantic Coast Pipeline**

By Maya Weber

Environmental groups are turning up pressure on the US Fish and Wildlife Service to more thoroughly vet the impacts of the Atlantic Coast Pipeline on vulnerable species, as the agency works to remedy a key permit for the natural gas pipeline project that has been struck by the US Court of Appeals for the 4th Circuit.

A Southern Environmental Law Center letter to FWS calling for further study was made public Tuesday, along with internal agency communications the group contends suggest political interference in prior decisions about the pipeline .

The action on behalf of several environmental groups comes as Dominion Energy has recently said it expects to see the authorizations reissued soon and construction back underway. Dominion could not be reached for comment Wednesday.

The 600-mile, 1.5 Bcf/d pipeline would take Appalachian gas to downstream markets in the Mid-Atlantic and is targeted for a late 2019 start.

Construction is currently paused under an order from the Federal Energy Regulatory Commission , issued after the 4th Circuit struck federal authorizations for the pipeline to cross under the Blue Ridge Parkway and an FWS "incidental take statement" setting permissible levels of harm to endangered or threatened species.

FERC has since asked FWS to restart a formal Endangered Species Act consultation.

Jeopardy determination

SELC argues data collected this summer show the project could jeopardize the continued existence of two species, and that FWS needs to consider alternatives including route modifications.

The group, which cast the original FWS analysis as suffering from a "rushed timeframe," highlighted agency emails suggesting the length of the original consultation in 2017 was compressed from the usual 135 days to 75 days.

The environmental group also highlighted emails dating back to April 2017 in which FWS career staff were admonished for offering comments on a draft environmental impact statement directly to FERC without giving political appointees a chance to review them.



"We ask that FWS base its evaluation on the project on the best available science, as the Endangered Species Act requires, removed from political winds," the environmental group said in its letter to FWS.

#### Bee surveys

Specifically, SELC pressed for surveys of the rusty patched bumblebee, an endangered species recently found to have more occurrences around the pipeline route than originally assumed.

"One of the most glaring shortcomings of the [FWS] biological opinion is the lack of data concerning the rusty patched bumblebee," the group argued, criticizing FWS' original analysis for relying on one hour of surveying on one road. Adequate surveying across the landscape is essential, it argued, because of new sightings of about 20 bees this summer by Virginia officials outside FWS' original "high potential zone."

#### Agency documents

SELC also turned to agency documents to show US Forest Service staff in July 2017 saw the potential for more of the bees to be present on national forest land. SELC also contended a conclusion about whether the project would jeopardize the species' survival appeared to be based on an analysis that was "reverse engineered."

"Ultimately, FWS decided a colony may be crushed by the project, yet that too did not change its determination, a conclusion at least some agency staff believed stood out 'like a hanging chad,'" the SELC letter said.

As proposed, the group contends ACP will jeopardize continued existence of the bee through adverse impacts to "what may be one of the most important RPBB populations remaining."

SELC also argued that more data collected this summer shows the continued existence of a species of mussel known as the clubshell is also likely to be jeopardized by the project.

The Department of Interior did not respond to a request for comment.

Separately, Virginia regulators have extended a public comment period until September 21 for a state air permit for a compressor station for the project in Buckingham County, Virginia. A decision on the permit has been put off until the next meeting of the state Air Pollution Control Board on November 8-9.

[Return to Top](#)

#### S&P Global

September 12, 2018

### Delaware River Basin Commission asks FERC for say on pipeline work in watershed

By Sean Sullivan

The Delaware River Basin Commission asked federal energy regulators to modify a permit for PennEast Pipeline Co. LLC's 1.1-Bcf/d natural gas pipeline project to prohibit early construction activity within the Delaware River watershed until the commission has issued its own approval.

In an April 3 letter made public by an environmental group Sept. 12, the Delaware River Basin Commission, or DRBC, asked the Federal Energy Regulatory Commission to amend its

approval of PennEast to forbid tree felling, one of the first steps in pipeline construction, in the Delaware River Basin, including wetlands and the riparian areas of tributaries, until the river commission authorizes the project. The DRBC also asked for the same deference in approvals of all future projects in the area.

"The DRBC is concerned that the felling of trees for such projects months or years before essential DRBC and state approvals have been issued can cause unnecessary or long-term and potentially substantial impacts to water resources, particularly in the context of very large projects involving hundreds of river, stream and wetland crossings," commission Executive Director Steven Tambini wrote in the letter. The impacts he listed included erosion of banks and sedimentation in streams and rivers.

The Delaware River Basin Commission, composed of representatives of the four states that surround the Delaware River and the U.S. Army Corps of Engineers, is in the midst of a review of PennEast. In a separate matter, the body proposed a ban on hydraulic fracturing for producing oil and gas in the watershed.

PennEast, an almost \$1 billion pipeline project backed by subsidiaries of Enbridge Inc., Southern Co., UGI Corp. and New Jersey Resources Corp. and by South Jersey Industries Inc., would run about 120 miles from northeastern Pennsylvania to New Jersey. FERC approved the project in January and rejected challenges to that decision Aug. 10. (FERC docket CP15-558)

PennEast spokeswoman Pat Kornick said the company would proceed within the limits of its authorizations.

The conservation group Delaware Riverkeeper Network obtained the letter from the Delaware River Basin Commission through a Freedom of Information Act request. The group said the letter did not appear in the PennEast docket at FERC, and the group did not find a response from FERC. FERC had not responded to questions about the letter by press time. The commission typically does not comment on active proceedings.

Delaware Riverkeeper, which has opposed PennEast with other organizations, has urged the Delaware River Basin Commission in petitions to use its authority to prevent construction, including tree clearing, before the commission issues its final decision.

"The DRBC taking such a strong and principled stance is an important development," Maya van Rossum, the Delaware Riverkeeper and leader of the Delaware Riverkeeper Network, said in a Sept. 12 statement. "We support the DRBC and the four states that are the commissioners in advancing this request."

[Return to Top](#)

Stateimpact.npr.org  
September 12, 2018

## **FERC urged to block tree-cutting before final decisions on PennEast pipeline**

Interstate agency fears 'unmitigated' damage unless pipeline is actually built

Jon Hurdle

The Delaware River Basin Commission asked a federal regulator to prevent PennEast cutting trees in the basin before it issues any approval for its controversial natural gas pipeline project in Pennsylvania and New Jersey, according to documents released on Wednesday.

But its request was not considered by the Federal Energy Regulatory Commission because it was not sent through the proper channels, a FERC spokeswoman said. The DRBC confirmed it had asked FERC to block early tree clearing by PennEast but had not received a reply.

Tamara Young-Allen, a spokeswoman for FERC, said the DRBC's request has not been considered because the letter was not sent to the agency's secretary, Kimberley Bose, as required, but to an official in the Office of Energy Projects.

If DRBC resubmits the letter through the proper channels, its request will be considered, Young-Allen said.

The documents were published by the environmental group Delaware Riverkeeper Network, which earlier this year urged DRBC to stop PennEast from doing any construction-related activities, including tree-cutting, until the interstate agency decides whether to issue permits.

In a letter to FERC in April, DRBC asked the agency to amend its certificate approving PennEast so that the company could not cut trees in the basin "until such time as the DRBC issues an approval for the project or activity."

DRBC, which represents the basin states of Pennsylvania, New Jersey, New York and Delaware plus the federal government, said it anticipates that PennEast might want to start cutting trees early in view of the many months it would take to build the 120-mile pipeline.

"The DRBC is concerned that the premature felling of trees could result in water resource impacts related to stream bank stability, soil erosion, and instream sedimentation that could go unmitigated unless and until the pipeline is actually built," the agency said.

The agency's request recalls Constitution Pipeline's felling of several acres of maple trees on a northeast Pennsylvania farm in 2016 to make way for a pipeline that failed about a month later to get a crucial permit from New York state. That project now appears to be dead after a series of judicial and regulatory setbacks, while the landowners, the Holleran family, [are seeking compensation for their lost trees](#).

Riverkeeper network head Maya van Rossum praised the river basin commission for asking FERC to deny any plans for tree clearing. She said DRN wants to avoid a repetition of the Constitution "debacle" but is also trying to remove one argument that FERC may use to overturn legal opposition to pipeline projects.

If trees are already cut, FERC may argue in court that a project is too far along to be denied, and seek to block all legal challenges, she said.

"We don't want any undue and/or premature damage inflicted and we don't want to see any undue pressure placed on the agencies because work has already begun in earnest on a project before all decisions are made," van Rossum said.

Pat Kornick, a spokeswoman for PennEast, declined to say whether the company plans to cut trees before getting any DRBC permit, but appeared to leave open that possibility.

"At the appropriate time, PennEast will proceed within the limits of the approvals that have been granted," she said.

PennEast anticipates beginning construction in 2019, Kornick said, later than its earlier plan for 2018.

FERC approved the project in January, but it still needs permits from the DRBC and the New Jersey Department of Environmental Protection. Those agencies could come under more pressure to approve the project if the company cuts trees before they have decided whether to issue permits, van Rossum said.

The project also needs approval from a federal judge in New Jersey who is deciding whether to grant the company's eminent domain petitions on about 150 landowners who declined offers of compensation for building the pipeline on their properties.

Van Rossum said DRN obtained the DRBC letter through a Freedom of Information Act filing with the agency.

[Return to Top](#)

S&P Global Platts  
September 12, 2018

## Pennsylvania landowners cite inactivity in asking FERC to rescind Constitution Pipeline permit

By Harry Weber

Williams said Wednesday it remains committed to reviving its Constitution Pipeline even as it faces a renewed property rights challenge from a group of Pennsylvania landowners and a roadblock in New York over a water permit.

The natural gas project is seen as important for alleviating bottlenecks in the pipeline - constrained US Northeast, home to the Marcellus and Utica shales .

New England , in particular, is heavily reliant upon pipeline imports from Canada and LNG imports from overseas to meet winter peak demand, factors that can increase prices during shortages. For four years since it received its US Federal Energy Regulatory Commission permit certificate, Constitution has been unable to initiate pipeline construction because of challenges from state officials, landowners and environmental groups.

“We continue to believe that the project should be allowed to proceed with construction,” Williams spokesman Christopher Stockton said in an email responding to questions. “The project represents much-needed energy infrastructure designed to bring natural gas to a region of the country that this past winter experienced the highest natural gas prices in the world.”

The latest hurdle stems from complaints from the owners of a 23-acre-property in New Milford Township, Pennsylvania that is to be crossed by the 121-mile pipeline and related facilities extending from two receipt points in Susquehanna County to a proposed interconnection in Schoharie County, New York .

Over the objection of the Holleran family and dozens of other landowners and community/environmental organizations, FERC issued the permit certificate for the project in 2014. A judge later granted the operator the right to seize a 1.84 acre right of way and 3.33 acre construction easement across the landowners' property to install the portion of the pipeline facilities that would cross it. To date, because of the inability to obtain a water permit in New York , Williams has only be able to fell trees on the property.

In June, the Holleran family asked FERC to rescind the permit certificate because Constitution wanted an additional two-year extension to complete construction. In a letter to FERC dated Tuesday, lawyers for the landowners renewed their request.

Among other things, they argue that absent a waiver by the commission, the project must have a permit from New York under Section 401 of the Clean Water Act to proceed with

construction. Since the state has denied the water permit and FERC has refused to grant a waiver, the landowners argue that the commission's permit certificate is invalid.

"The commission is only authorized to issue certificates for projects capable of 'construction and operation,'" the letter said. "Because the project approved can no longer be built and is no longer jurisdictional, the commission must rescind the certificate immediately."

The landowners also want certainty over their property given the length of time the easement has been in effect.

"It has been over three and a half years since the Hollerans' property was taken for this project, and over two years since a swath of 558 trees were razed through the wooded area on their property," the letter said. "The Hollerans are now in federal court seeking return of their property and payment of compensation for full restoration of their property, loss of their business, attorneys' fees and intentional infliction of emotional distress."

Stockton said the certificate of public convenience and necessity issued by FERC for Constitution is still in effect, and the project's sponsors remain committed to the project. Shippers include Cabot Oil & Gas and Duke Energy's Piedmont Natural Gas.

#### Protracted fight

In filings responding to the landowners' earlier claims, Williams said it has not exhausted all of its remedies for securing a waiver of the New York water permit and, as such, the project is still viable.

"Contrary to the arguments of the Holleran landowners, which fail to cite any cases where the commission's jurisdiction of a project was vacated while proceedings related to the certificate order for that project were pending before the commission, as is the case here, the certificate order clearly continues to authorize the project," the operator argued.

On July 19, FERC rejected a request by Williams that the commission reconsider its finding that the New York State Department of Environmental Conservation acted appropriately under the Clean Water Act when it denied the water permit to the 650 MMcf/d pipeline project.

At the time, Williams said the final FERC decision would allow the project developer to ask a federal appeals court to review it. Stockton said Wednesday a 60-day window to appeal FERC's denial of a rehearing closes next week. He reiterated that the operator plans to appeal.

[Return to Top](#)

## Congress

E&E Daily  
September 13, 2018  
APPROPRIATIONS

### Senate approves energy and water bill

[George Cahlink](#), E&E News reporter

Congress is expected to send the president a fiscal 2019 Energy-Water spending bill that's part of a bipartisan, \$147.5 billion funding package after the House approves it today.



Last night, the Senate passed the three-bill spending minibuss 92-5, the wide margin signaling support for averting a government shutdown when the new fiscal year begins on Oct. 1.

The package contains the fiscal 2019 Energy-Water, Military Construction-Veterans Affairs and Legislative Branch bills ([E&E Daily](#), Sept. 12).

The White House has not objected to the package, although there is uncertainty over whether President Trump will support any new spending without a guarantee of border wall funding.

Senate Appropriations Chairman Richard Shelby (R-Ala.) said it was his expectation that the minibuss would quickly become law.

That would validate the push by congressional leaders to move multiple bills in packages to get as many signed into law before the new fiscal year. The approach has required both parties to control their desire for partisan policy riders and hold off on funding fights.

House and Senate appropriators are set to conference today on two more minibuss packages. One would combine the Interior-EPA bill with funding for Agriculture, Transportation-Housing and Urban Development, and Financial Services.

The other would marry up the annual Defense bill with the largest domestic measure, Labor, Health and Human Services, and Education.

Shelby said negotiations over the Labor-HHS-Defense bill could be finalized and the bill could be on the Senate floor next week.

Asked about the Interior-EPA bill, Shelby was more circumspect about when it might reach the floor, saying "stay tuned."

He noted that if only the first two spending minibusses were approved by Oct. 1, they would still cover about 80 percent of all federal discretionary spending.

Both Republican and Democratic aides say the Interior-EPA funding measure might not be wrapped before the new fiscal year, in part because lawmakers are haggling over various environmental provisions.

Sen. Tom Udall (D-N.M.), the ranking member on the Senate Interior and Environment Appropriations Subcommittee, was more optimistic yesterday that a deal would soon emerge. He said negotiators were "making good progress" and that he thought the riders could be resolved.

Any agencies not receiving fresh dollars by Oct. 1 are expected to be funded under a stopgap spending measure, known as a continuing resolution, that would guarantee them level funding until after the elections.

Lawmakers are eager to move a CR rather than risk a shutdown before the elections — even as Trump has not entirely ruled one out.

The House's No. 4 Democrat, Rep. Joe Crowley of New York, told reporters yesterday that his party opposes a shutdown and made clear it would blame the GOP if one were to occur under Trump's watch.

"We don't believe that's in the interest of our constituents or of the country to see that happen. And our hope is that our Republican colleagues will see that as well, work with us. But certainly, the responsibility is upon them," he said.

Reporter Geof Koss contributed.

Twitter: [@GeorgeCahlink](#) Email: [gcahlink@eenews.net](mailto:gcahlink@eenews.net)

[Return to Top](#)

## States

Energywire  
September 13, 2018  
UTILITIES

### Worst-case scenario plans in place as Florence bears down

[Kristi E. Swartz](#), E&E News reporter

Duke Energy Corp. officials said as many as 75 percent of its customers in North and South Carolina could lose electricity during Hurricane Florence, and some should expect to be without power for weeks.

That would be the worst-case scenario should the storm hit Wilmington and then move through all three of North Carolina's major metropolitan areas. Right now, Florence is on more of a westward path after it hits land, which could spare many of those customers.

"The plan we're putting in place is for the worst-case scenario," which means up to 3 million residents and businesses lose electricity, Howard Fowler, Duke's storm director, said during a media briefing yesterday.

Duke has more to worry about than power outages and potential damage to its grid. There is concern that its coal ash ponds could flood, releasing toxic materials into rivers and streams and eventually affecting drinking water.

At least one of Duke's nuclear plants could face hurricane-force winds, as well, which means it must be shut down beforehand per federal safety regulations.

The Mid-Atlantic is bracing for what officials are calling a catastrophic event as Florence bears down on the coast. The storm is expected to hit the Carolina coast tomorrow. It is currently a Category 2 storm but is expected to strengthen again.

As with most storms, Florence has been unpredictable. It was poised first to go directly across North and South Carolina, but models on Tuesday night started showing the storm moving westward into Georgia before fanning out into Tennessee, Kentucky and parts of western North Carolina.

All of the region's electric utilities had been watching Florence for more than a week, but the hurricane's latest shift meant Southern Co.'s Georgia Power Co. and the Tennessee Valley Authority had to take more notice.

Georgia Gov. Nathan Deal (R) declared a state of emergency yesterday. Georgia Power is also keeping all of its crews in the Peach State until it is clear that they are not needed and can go help other electric companies if necessary.

Southern's Alabama Power and Gulf Power continued to send their crews to the Carolinas as their home territories are not likely to be as affected.

Fowler at Duke said more than 9,400 crews are coming to help, with some traveling as far as Texas. That is in addition to 1,700 workers traveling from Duke's Midwestern territory and 1,200 from Duke Energy Florida.

Duke has assembled the largest number of tree, damage and line crews — 20,000 total — in

its history, said David Fountain, president of Duke Energy North Carolina.

"We're anxious to get to work," he said.

It's still unclear when that will be. Although Florence's winds combined with the storm's size will pack a strong punch, its sluggish speed and rain will be the largest threat.

#### Coal ash risks

Florence is crawling to the coast, and forecasters expect it to stall once it gets there. This means much of the Carolinas could flood, and it will take Duke longer to be able to safely assess equipment damage and get to work.

Officials warned that they expect to have a lot of equipment underwater, and any power lines that already are underground will be difficult to get to.

This also means its sister company, Piedmont Natural Gas Co. Inc., has had to prepare for the potential of underwater meters, gas appliances and other equipment, Fountain said.

A chief concern is the 31 coal ash basins at Duke's coal-fired plants in North Carolina. Half of those 14 coal plants are shuttered, but the basins remain.

Fountain said the levels of water in those basins were lowered already as the utility moves through its program to close them. Crews are inspecting the ponds ahead of the storm and will do so again once it passes, he said.

"There's plenty of capacity in those ash basins if we have the type of flooding that we're expected to have here," he said. If there is more water than the basins can handle, then Duke will take steps to minimize coal ash overflowing into nearby rivers, he said.

Duke's bigger concern is rivers and creeks that are likely to flood and flow into cooling water intake ponds that are at those coal plants, Fountain said. Those ponds do not have coal ash or any other toxic chemicals in them, he added.

Officials from Georgia Power and TVA said they will monitor their ash sites but that they are designed to withstand severe weather.

#### Nuclear flooding hazards

The amount of flooding at the region's nuclear plants is a red flag for the Union of Concerned Scientists, which argues that the high waters put at least two sets of reactors in North Carolina and Virginia in harm's way.

Duke's Brunswick plant near Wilmington and Dominion Virginia Power's Surry plant near Williamsburg are particularly vulnerable in this case, UCS said in a news release yesterday.

"Nuclear plants are safe from flooding if plant operators properly install protective measures and designers accurately forecast flooding hazards," said Edwin Lyman, a senior scientist in the UCS Global Security Program and an expert in nuclear plant design. "Falling short on either requirement would make a nuclear plant more vulnerable to floods, which could lead to a meltdown."

The U.S. Nuclear Regulatory Commission has sent inspectors to reactors in North and South Carolina and Virginia. Reactors have to be shut down roughly two hours before sustained hurricane-force winds are expected to hit the area.

Meteorologists are predicting that Florence's storm surge could be as high as 13 feet, UCS said.

Fountain stressed that Duke's nuclear workers are trained and prepared to secure the reactors

during a hurricane.

Georgia Power's nuclear reactors likely won't face hurricane-force winds, but its Vogtle nuclear expansion project is an active construction site. The utility continues to monitor Florence for any potential impact to the site and has plans in place to ensure the site and employees remain safe before, during and after the storm, spokesman Jeff Wilson said.

Flooding is a chief concern across the Tennessee Valley, where TVA operates 49 dams. TVA keeps the water level higher in the summer, but heavier-than-normal rain in the spring and summer also contributed to that, said James Everett, senior manager of TVA's River Forecast Center in Knoxville.

The public power utility, which serves seven states, usually starts to release water in the fall and winter. Florence has accelerated that.

"We're getting a little bit more aggressive on the releases," he said.

The challenge now is that TVA — and everyone else — is getting revised rainfall information roughly every six hours, Everett said. That means it must watch its entire territory and change its water-release strategy if needed.

TVA is sending roughly two-thirds of its construction crews to North Carolina today. It is also sending two helicopters, pilots and a mechanic to Charlotte, where they will ride out the storm in a hangar before helping Duke.

Twitter: [@BizWriterKristi](#) Email: [kswartz@eenews.net](mailto:kswartz@eenews.net)

[Return to Top](#)

**S&P Global**  
**September 12, 2018**

## **Duke Energy 'ready to attack' Florence, forecasts up to 3 million outages**

By Darren Sweeney

Duke Energy Corp. said it is "well prepared" for the major hurricane churning toward the coast of the Carolinas but anticipates up to 3 million customers could lose power with restoration taking weeks.

"The Carolinas are clearly in the crosshairs for Florence and preparations, such as evacuations, are well underway," Duke Energy North Carolina President David Fountain said Sept. 12 on a conference call with reporters. "As Florence nears the Carolinas, the forecast increasingly shows this is likely to be a historic storm, leaving historic damage in its wake."

Hurricane Florence weakened slightly to a Category 3 hurricane with maximum sustained winds of 125 miles per hour, according to the 2 p.m. ET advisory from the National Hurricane Center on Sept. 12.

Still, Fountain warned the storm is projected to hit the Carolinas as a "powerful major hurricane" that could stall along the coast just after making landfall.

"Based on the latest track and overall forecasts for Florence, our modeling projects we expect to see somewhere between 1 [million] and 3 million outages for the 4 million homes and businesses that we serve," Fountain said, noting 25% to 75% of the company's customers in the Carolinas could lose power.

"It is important for customers and people to know though that this is no ordinary storm,"

Fountain said. "People could be without power for a very long time. Not days, but weeks."

Duke Energy warned it may not be able to reach locations for several days because of heavy rains and flooding with "lingering winds" making it difficult to complete damage assessments.

Howard Fowler, Duke Energy's incident commander for the Carolinas, said the company has more than 20,000 people in place to help restore power. Duke Energy has been bringing in crews from its Midwest and Duke Energy Florida LLC service territories to assist with storm preparation, while also coordinating with other utilities throughout the Southeast.

"We are ready to attack this storm and restoration ... when it is safe to do so," Fowler said.

The company also expects the hurricane to impact its natural gas infrastructure and service.

"While not nearly to the same extent as the electric system, it will likely still be a major work effort for our gas teammates here at Duke Energy and [Piedmont Natural Gas Co. Inc.]," Fountain said.

Duke Energy, which operates in North Carolina and South Carolina through Duke Energy Carolinas LLC and Duke Energy Progress LLC, also is shoring up its ash basins and power plants ahead of Florence. This includes staging staff and equipment at the sites closest to the coast, while lowering leachate levels at landfills.

Duke Energy uses drones to access locations that are hard to reach by land or boat and has emergency action plans in place that include steps for notifying emergency management partners.

#### Nuclear risk

Duke Energy's nuclear plants in the Carolinas would be required to shut in advance of the arrival of winds of more than 73 miles per hour, Karen Williams, a spokeswoman for the 1,928-MW Brunswick plant near Wilmington, N.C., said. The units would have to be shut at least two hours before the arrival of hurricane-force winds, she added.

The same requirements apply to most U.S. nuclear units. Nuclear reactors are protected against extreme winds, including tornado-strength gusts, but shut as a protective measure in case off-site power is lost.

The Carolinas have 12 of the country's 99 nuclear units. In addition, there are four units in Virginia and two in Maryland.

SCANA Corp. subsidiary South Carolina Electric & Gas Co. is also prepared to shut its 992-MW V.C. Summer station in Jenkinsville, S.C., spokeswoman Rhonda O'Banion said. The utility is evaluating whether it will need to increase staffing levels before the storm, she said.

"Regardless of this storm's exact path, we anticipate Florence will bring dangerous winds and the potential for heavy rain and flooding across our service territory, which could result in significant power outages for our customers," South Carolina Electric & Gas Vice President of Operations Bill Turner said in a news release on Sept. 10. "We have worked for years to strengthen our system against the impacts of severe weather, and our response for this particular event has already begun."

Dominion Energy Inc. subsidiary Dominion Energy Virginia, known legally as Virginia Electric and Power Co., and Exelon Corp.'s Baltimore Gas and Electric Co. also issued news releases about their storm preparatory efforts.

If Dominion's costs are significant, the Virginia State Corporation Commission provides two methods to recover them: a base rate increase or a charge against earnings during a financial review, commission spokesman Ken Schrad said in an email Sept. 11.



Dominion Energy Virginia owns and operates the 1,750-MW Surry nuclear plant in southeastern Virginia, which also could be impacted by Florence.

S&P Global Platts reporters William Freebairn and Mark Watson contributed to this article. S&P Global Platts and S&P Global Market Intelligence are owned by S&P Global Inc.

[Return to Top](#)

**S&P Global Platts**  
September 12, 2018

## **US STORM: Utilities expect massive outages, high repair costs from Florence**

By Mark Watson

As Hurricane Florence approached the Atlantic Seaboard and a tropical disturbance looked increasingly likely to become a cyclone threatening the US Gulf Coast , power companies shifted thousands of workers toward likely trouble areas, and industry observers pondered a future with grids fighting disasters on multiple fronts.

Duke Energy meteorologists on Wednesday said power outages from Hurricane Florence could range between 1 million and 3 million customers.

"The magnitude of the storm is beyond what we have seen in years," said Howard Fowler, Duke Energy 's incident commander. "With the storm expected to linger, power restoration work could take weeks instead of days."

Duke is bringing in more than 20,000 people to restore power — the company's largest-ever resource mobilization. More than 8,000 Carolinas-based workers are being joined by 1,700 workers from Duke Energy Midwest and 1,200 from Duke Energy Florida to respond to this storm. Another 9,400 workers are coming from other utilities to help.

Among those are about 100 people each from Entergy Arkansas and Entergy Mississippi , but Entergy Texas is keeping its crews on standby as the National Hurricane Center gives a tropical disturbance located in the central Gulf of Mexico a 70% chance of becoming a cyclone by Friday afternoon.

"Regardless of development, heavy rainfall and gusty winds are expected across portions of northeastern Mexico , Texas , and Louisiana late this week," the National Hurricane Center said.

Another utility that has not yet moved repair workers in preparation for the storm is Georgia Power, as Florence's forecast path has moved south to encompass more of that state.

Georgia Power spokeswoman Meredith Stone said, "We are holding our crews in place until Florence makes landfall and we know where they are needed."

### **Nuclear complications**

One issue that complicates the situation may be the high concentration of nuclear power along the potential impact areas.

Duke's 1,928-MW Brunswick plant is on a coastal area near Southport, North Carolina , that could face a 20-foot storm surge, with as much as 40 inches of rainfall, and the storm surge alone could cause flooding at the plant, according to S&P Global Platts Analytics. Also, the

973-MW Shearon Harris plant is in an area southwest of Raleigh, North Carolina , that is most likely to be affected by severe flooding, but the region has 10 other nuclear plants near the coast that may be at risk.

Another plant at risk is the 1,750-MW Surry nuclear plant near Williamsburg, Virginia , according to a statement from the Union of Concerned Scientists, which also cited risks at the Brunswick plant.

Dave Lochbaum, UCS nuclear safety project director, said, "We do know that both Brunswick and Surry have had potentially serious problems that we hope they fixed."

The US Nuclear Regulatory Commission in March 2017 said the Brunswick plant's buildings were estimated as capable of handling a storm surge of up to 7 feet at the reactor buildings, while the Surry plant's greater risks are flooding from heavy rainfall that could top the plant's barriers, the UCS statement said.

#### Disastrous economic effects

Therefore, the repair costs from Hurricane Florence may be large — some estimates have ranged from \$20 billion to \$30 billion for all types of damage, not just utilities . In comparison, restoration costs from Hurricane Harvey, which struck Texas and Louisiana over the Labor Day weekend in 2017, were estimated to total \$125 billion.

The White House estimated Harvey's cost to the US economy at 0.6 percentage point off the annual GDP.

Matthew Cordaro, a former Midcontinent Independent System Operator CEO who now resides in New York , noted that local communities "are usually impacted over an extended period of time" after such a disaster.

"On the other hand, utilities have the potential to recover relatively quickly because they ultimately are guaranteed return of their costs from ratepayers," Cordaro said.

Platts Analytics estimated that it took 10 days for power demand to be restored to normal after Hurricane Harvey, but that the stronger Hurricane Florence may cause demand declines to persist longer than recent examples.

Carey King, University of Texas Energy Institute assistant director, said power companies' capital costs "are already increasing in an absolute sense and per customer ... more than just because of destroyed infrastructure."

For investor-owned utilities and others that report to the US Federal Energy Regulatory Commission , capital costs for all purposes have increased from less than \$750/customer in the early 2000s to about \$1,000 in 2017, King said.

Scott Miller, executive director of the Western Power Trading Forum, said, "It has been suggested that climate change is making this job more frequent and thus more expensive. Probably true.

"Utilities have always done well, and will continue to do well" in managing service restoration, but if disasters strike more frequently, utilities that have been getting less revenue based on energy sales have fewer resources to prepare and respond.

"However, getting regulators to recognize there is a need to 'harden' distribution systems (usually the culprit in outages) could be a cost-effective investment that regulators could allow, which would replace the lost investment 'growth' from generation," Miller said. "This is probably the future."

[Return to Top](#)

S&P Global Platts  
September 12, 2018

## Hurricane Florence expected to dampen gas demand in US Southeast

By Jim Magill ,John DeLappJason Lord ,Veda Chowdhury ,Tyler Jubert

Hurricane Florence, which is forecast to make landfall along the coast of North Carolina later this week, is expected to reduce natural gas demand across a wide swath of the southeastern US , although its current track makes it less likely that the storm will impact gas production or demand in the Appalachia region.

As of Wednesday afternoon, the National Hurricane Center predicted that after making landfall, the storm will produce torrential rain that would inundate all of South Carolina , a large part of North Carolina , as well as parts Alabama , Tennessee , Kentucky and Virginia .

Although Florence is predicted to reach into southern West Virginia several days after making landfall, it is not expected to extend to the producing region in the north of that state.

### Demand destruction seen

Because of its strength — Florence is on track to be the strongest hurricane to ever hit the US Southeast — it is difficult to predict the storm's potential to cut gas demand in the region.

The most recent comparison to be made is Hurricane Arthur, which slammed into the North Carolina coast as a Category 2 storm in July 2014.

During this storm, sample demand in North Carolina , South Carolina , Georgia and Virginia fell by a combined 1.8 Bcf /d between July 1 and July 4, 2014, to 3.4 Bcf /d, according to Platts Analytics data. Since most of this fluctuation in demand came from power plants, it's likely that the temperature drops seen during the storm resulted in lost demand for gas .

In the four years since Arthur touched down, demand across North Carolina , South Carolina , Virginia and Georgia has increased, with total sample for the four states upwards of 6.3 Bcf /d over the last 30 days, offering more downside risk to demand.

### Utility advisories

Gas utility companies across the Southeast issued advisories warning of possible outages of both gas and power in the region.

South Carolina Electric & Gas , which serves a 22,000-square-mile territory in South Carolina , said it plans to deploy about 2,900 personnel to respond to power outages following the storm.

In a statement, the SCANA subsidiary predicted that the storm would “bring dangerous winds and the potential for heavy rain and flooding across our service territory, which could result in significant power outages for our customers.”

Piedmont Natural Gas , which distributes gas to more than 1 million residential, commercial and industrial customers and power plants in North Carolina , South Carolina and Tennessee , said it was launching its severe weather preparedness plan. The Duke Energy subsidiary issued a list of safety recommendations for customers who experience flooding or any other damage

to their gas equipment or appliances as the result of Hurricane Florence.

#### Prices

With Hurricane Florence still at sea Wednesday, gas prices remained largely unaffected by the storm, according to Platts pricing data.

With the US National Weather Service's track for Florence showing the storm taking a more southerly turn than previously forecast, the biggest price impact is likely to be seen in the Southeast and will likely come Thursday, when trades are made for delivery the following day.

Transco Zone 5 delivered, a Platts pricing point that runs through the Carolinas and Virginia, was unchanged at \$3/MMBtu.

Florida Gas Transmission Zone 3 rose 6.5 cents to \$3.04/MMBtu Wednesday.

On Friday, deals will be done for delivery through the weekend, a time when demand is typically lower than during the workweek. That consumption could be down even further due to the storm.

Price impacts from the storm are less likely to be felt in the Appalachian gas-producing region. Dominion South, an Appalachian pricing point that mostly tracks gas prices in West Virginia, was trading at \$2.23/MMBtu Wednesday after falling 7 cents.

[Return to Top](#)

#### Greenwire

September 12, 2018

HURRICANE FLORENCE

### Carolinas race to bolster fragile dams

[Jeremy P. Jacobs](#), E&E News reporter

As Hurricane Florence barrels toward the East Coast, state regulators are rushing to safeguard a historically fragile piece of the Carolinas' infrastructure: dams.

North Carolina and South Carolina have been home to some of the most significant recent dam disasters due to hurricanes and major rain events.

In October 2015, torrential rains in Columbia, S.C., caused 51 dams to fail. A year later, Hurricane Matthew made landfall on the South Carolina coast, and another 25 dams breached.

Matthew had a similar impact on North Carolina as at least 17 dams gave way.

Those disasters caused tens of billions of dollars in property damage, and dozens of lives were lost.

But there was a silver lining. Those disasters led the states to beef up their dam safety regimes.

"This keeps happening to them, so they have ramped up their staffing and they have quite a bit more budget," said Mark Ogden of the Association of State Dam Safety Officials, referring to South Carolina.

"There is good reason to believe that they are a lot more prepared and ready for this type of event," Ogden said.

South Carolina's program underwent an extreme makeover after the 2015 and 2016 storms. As recently as 2010, the Department of Health and Environmental Control's Dams and Reservoirs

Safety Program had just one full-time employee that was responsible for the state's roughly 2,400 dams.

Like most of the country's 90,500 dams, most of South Carolina's are relatively small — less than 25 feet — and privately owned. But even those dams, which are frequently used to create recreational lakes, can cause major damage.

Dams are given a hazard rating based on how destructive a failure would be. "High" means a breach would result in the loss of life. "Significant" indicates major property damage but no fatalities.

In the 2015 storm, a series of earthen structures broke open sending a deluge down the Gills Creek watershed northeast of Columbia. In some cases, the owners of the dams didn't know they were responsible for them. In others, the state couldn't find the owner.

South Carolina's traditionally conservative state Legislature soon thereafter voted to boost the dam safety program. It received an influx of funding and now has roughly a \$1.1 million budget and more than 20 full-time employees ([Greenwire](#), April 10, 2017).

The program has worked to make sure all dams have an emergency action plan, or EAP, which set out what to do when hurricanes like Florence hit.

According to the Army Corps of Engineer's National Inventory of Dams, nearly all of South Carolina's high and significant hazard plans have EAPs, which is unusual.

The Association of State Dam Safety Officials is, coincidentally, holding its annual dam safety conference this week in Seattle. Ogden said South Carolina's team, which is highly regarded because of the strides they have made, didn't come. They stayed home to prepare for the storm.

Earlier this week, the department directed dam owners to check their dams and begin lowering water levels to make room for rain from the upcoming storm.

"Owners of reservoirs with functional gates or flashboards should consider operating them to provide additional storage for the anticipated rainfall," said Jill Stewart, director of the state's dam safety program, in a statement.

North Carolina is taking similar precautions. Ogden said the Tarheel State has had a robust dam safety program for several years, with more than 20 employees and a roughly \$2.2 million budget. Those officials left the conference early this week.

North Carolina has about a thousand more dams than South Carolina, 3,444, and a higher percentage that are high hazard, 1,448, or 42 percent. Like its southern neighbor, most are private and built in the 1950s, '60s and '70s.

According to the National Inventory of Dams, fewer of North Carolina's high and significant hazard dams have EAPs. About 43 percent of its high hazard dams have the plans, while 10 percent of the significant hazard dams do.

Ogden cautioned that those numbers are slightly outdated and that North Carolina has made strides in recent years to improve them. He said that roughly half of the state's high hazard dams now have the plans and the state has implemented new safety requirements.

"But it's still a concern that some their dams don't have them," he said.

Bridget Munger, a spokeswoman for North Carolina's Department of Environmental Quality, said their Dam Safety Program is working to prepare dam owners for the hurricane.

The program has personnel in seven regional offices monitoring dams that have been



identified as having structural or other deficiencies, or undergoing repair and construction.

They have also been contacting dam owners and, like South Carolina, telling them to consider lowering water levels.

"As with Hurricane Matthew [in 2016] and severe storms before that, DEQ personnel are prepared to respond immediately should a dam emergency occur," Munger said.

There are also a few dams potentially in Florence's path that are federally controlled. The Army Corps of Engineers operates no dams in South Carolina, but has three in North Carolina — the Falls Lake, B. Everett Jordan and W. Kerr Scott dams — as well as two in Virginia and one in Maryland.

The Army Corps "has fully-engaged teams actively monitoring and managing these dams to make as much water storage available as possible," spokesman Pete Pierce said in an email. "These dams reduce the risk of downstream flooding, but do not eliminate it. Risk remains from the potential massive rainfall and flooding downstream from other drainage areas not associated with the dams."

Of course, a robust dam safety program and these precautions don't mean the expected record precipitation and wind from Florence won't overwhelm dams. Last year, Hurricane Harvey caused two dams near Houston to overflow for the first time in their history, though the dams technically did not fail.

And Hurricane Maria caused a failure of a spillway at Puerto Rico's 90-year-old Guajataca Dam, forcing the evacuation of 70,000 downstream.

Environmental groups such as American Rivers have said the recent disasters in the Carolinas show that outdated and unsafe dams should be removed and that state dam safety laws and programs need to be even further strengthened.

Michael Connor, former deputy secretary of the Interior Department and Bureau of Reclamation commissioner, said communication between state and federal authorities will be key.

"The potential record levels of precipitation will pose an incredible test for infrastructure in the Southeast and Mid-Atlantic areas, particularly dams in the region," Connor said.

"Coordination between federal, state, & local authorities on how these facilities are being operated throughout this event, and whether there are any safety issues given the extreme nature of the event, is another critical aspect of governments' overall response to the hurricane," he said.

Twitter: [@GreenwireJeremy](#) Email: [jjacobs@eenews.net](mailto:jjacobs@eenews.net)

[Return to Top](#)

**S&P Global Platts**  
September 12, 2018

## **Pa. lawmakers call for Mariner East work halt after blast on other ETP pipe**

By Bill Holland, S&P Global Market Intelligence

A bipartisan group of eastern Pennsylvania state lawmakers called for construction on Energy Transfer Partners' Mariner East 2 NGL pipeline to be halted immediately after the company's Revolution pipeline exploded in a rural area in the western part of the state on September 10.

The September 10 blast destroyed a house, a barn and several adjacent FirstEnergy electric transmission lines in Center Township, Butler County, authorities said. Automatic shutoff valves cut the flow of gas, and the fire burned itself out over several hours that morning, Energy Transfer Partners, or ETP, said.

State lawmakers representing parts of Delaware and Chester counties, outside Philadelphia, called for an immediate halt to ETP's work on the Mariner East 2 NGL line through their districts until ETP's Sunoco Pipeline affiliate proves a similar explosion in their more densely populated towns can be avoided.

"This area of Beaver County is far less dense than the pipeline corridor in Delaware County," Republican state Representative Chris Quinn said in a statement. "A similar incident in my district could be even more destructive and have a greater human toll."

"This pipeline should not be built until the real and legitimate safety and environmental concerns raised by myself and local residents have been fully addressed," Quinn said.

Two state senators from the area, Republican Thomas McGarrigle and Democrat Andrew Dinniman, echoed Quinn's objections. Dinniman filed a complaint in spring with the state Public Utility Commission, claiming that ETP had not lived up to its consent agreements. He called for a closer examination of the geology along the pipeline's route and improved coordination between ETP and local fire and police departments. An administrative law judge immediately suspended Mariner East 2 construction at 12 sites, saying ETP and Sunoco value speed over safety. That ban was lifted for eight sites in August.

ETP has also run afoul of Pennsylvania's environmental regulators and was assessed \$12.6 million in fines after repeatedly spilling drilling fluids into wetlands and streams over two years.

The Revolution explosion was the latest in a string of incidents that have resulted in fines, suspensions and public suspicion for ETP's Pennsylvania projects. At one point this past spring, a PUC administrative law judge halted all work on the Mariner East family of pipelines.

Revolution is a 100-mile, 24-inch-diameter header line connecting well gathering systems to ETP's larger Rover Pipeline for dry gas and Mariner East 1 and 2 for gas liquids such as ethane and propane.

[Return to Top](#)

**The Energy Daily**  
September 13, 2018

## **SCE proposes \$582 million plan to prevent grid-related wildfires**

Southern California Edison this week was the first to respond to a new state law requiring utilities to submit plans to reduce grid-related wildfires, asking state regulators to approve a \$582 million program to upgrade fire prevention across its transmission and distribution system.

The plan also is designed to reduce the utility's exposure to wildfire liability costs, which have soared into the billions of dollars for the state's three investor-owned utilities due to multiple huge blazes that have caused massive damage in communities across California in recent years.

In a Monday filing at the California Public Utilities Commission (CPUC), Southern California

Edison (SCE) said its grid safety and resiliency program will include replacing 600 miles of overhead power lines in high fire risk areas with insulated wire by the end of 2020, which the utility said would be the first large-scale deployment of insulated wire in the United States designed to reduce wildfire risk.

SCE also is installing 15,700 current limiting fuses, which interrupt current more quickly than traditional, industry standard fuses and are expected to boost reliability by segmenting circuits to isolate problems, thereby limiting the number of customers affected by an outage.

In addition, SCE said it will install additional remote-controlled automatic reclosers (RARs) on its system. Under normal conditions, the grid automatically tests any circuit experiencing a temporary fault. During “red flag” conditions of low humidity and high wind, SCE uses RARs to stop affected circuits from automatically re-energizing so crews can physically inspect the lines before they are re-energized.

The utility’s plan calls for a number of other projects to enhance “situational awareness.” It will install high-definition cameras, weather stations and modeling tools, while on the operations side, SCE said it will inspect all trees within 200 feet of its electric facilities and remove or prune trees that could strike the equipment.

The utility also is proposing a pilot project to deploy drones to quickly survey power lines so power can be restored more quickly after an emergency outage.

“The devastation caused by the 2017 and 2018 wildfires leaves no doubt that wildfire risk has increased to the point where California needs to reassess the way we collectively prepare for and prevent wildfires,” said Phil Herrington, SCE senior vice president for transmission and distribution. “This includes a role for utilities in going beyond existing state standards and traditional utility practices to incorporate leading mitigation measures....”

[Return to Top](#)

From: (b) (6)  
To: (b) (6)  
Date: Wednesday, September 12, 2018 9:03:00 AM  
Attachments: [ResilienceforGridSecurityEmergencies.pdf](#)

---

Hi (b) (6)

Wanted to forward you a recent report, *Resilience for Grid Security Emergencies: Opportunities for Industry-Government Collaboration*. This has a legal component that you may be interested in.

As noted by SANS:

A study published by the Johns Hopkins University Applied Physics Laboratory (JHUAPL) says that “before adversaries strike, power companies and government officials should partner to draft basic ‘template’ orders to defend the grid.to create a plan to respond to attacks against the country’s critical infrastructure.” The report suggests that when a physical or cyberattack on the power grid is detected, the White House should declare a “grid security emergency,” which would be followed by emergency phases of “imminent attack,” “attack is occurring,” and “restoration.”

Best,

(b) (6)

IT Specialist (INFOSEC)  
Office of Energy Infrastructure Security (OEIS)  
Federal Energy Regulatory Commission  
888 First St NE, Washington, DC 20426

(b) (6)

# RESILIENCE FOR **GRID SECURITY** EMERGENCIES

**Opportunities for Industry–Government Collaboration**

**National Security Perspective**



Paul N. Stockton

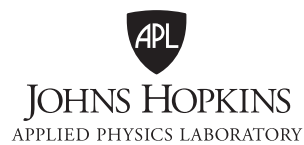




# **RESILIENCE FOR GRID SECURITY EMERGENCIES**

Opportunities for Industry–Government Collaboration

Paul N. Stockton



Copyright © 2018 The Johns Hopkins University Applied Physics Laboratory LLC. All Rights Reserved.

This National Security Perspective contains the best opinion of the author at time of issue. The views expressed in this study are solely those of the author and do not necessarily reflect the opinions, practices, policies, procedures, or recommendations of the US Department of Energy or any other US government agency or of JHU/APL sponsors.

## Contents

Figures.....	v
Summary .....	vii
<b>Developing Emergency Orders under the FPA.....</b>	<b>1</b>
Drafting Template Emergency Orders before Attacks Occur .....	3
Participants in Drafting and Implementing Emergency Orders .....	5
Goals and Specific Design Requirements for Developing Emergency Orders .....	11
<b>Threats, Thresholds, and Consultative Options for Declaring Grid Security Emergencies .....</b>	<b>13</b>
Threats That Can Trigger Grid Security Emergencies .....	13
Thresholds for Declaring Grid Security Emergencies .....	17
Data Sharing and Consultations with Industry .....	25
<b>Grid Security Emergency Phases and Order Design Options .....</b>	<b>28</b>
Preattack Options.....	29
Extraordinary Measures when Attacks Are Occurring.....	33
Emergency Orders to Support Power Restoration.....	35
<b>Additional Emergency Order Design Parameters and Supporting Initiatives .....</b>	<b>38</b>
Deterring and Defeating US Adversaries.....	38
Communications Requirements for Issuing and Employing Emergency Orders .....	46
The Deeper Value Proposition for Emergency Orders.....	52
<b>Conclusions and Recommendations for Broader Progress .....</b>	<b>58</b>
Employing Additional Emergency Authorities for Cross-Sector Resilience.....	59
Extended Partnership Requirements within the United States and Abroad.....	64
Playing Defense in Cyberwarfare .....	70
Bibliography .....	75
Acknowledgments.....	93
About the Author .....	93



Figures

Figure S-1. Grid Security Emergency Phases..... viii

Figure 1. Stakeholders for Building Grid Security Emergency Resilience.....10

Figure 2. ODNI Cyber Threat Framework.....20

Figure 3. Elements of the Cyber Incident Severity Schema .....21

Figure 4. Notional Decision Framework for Declaring Grid Security Emergencies.....26

Figure 5. Emergency Order Matrix: Examples of Order Designs .....29

Figure 6. Categories for Protecting Defense Critical Electric Infrastructure .....41

Figure 7. NERC Regional Entities across North America .....67

Figure credits:

Figure 2: “The Cyber Threat Framework,” ODNI (Office of the Director of National Intelligence), n.d., <https://www.dni.gov/index.php/cyber-threat-framework>.

Figure 3: DHS (US Department of Homeland Security), *National Cyber Incident Response Plan* (Washington, DC: DHS, December 2016).

Figure 7: Information from NERC (North American Electric Reliability Corporation), <http://www.nerc.com/Pages/default.aspx>; figure reprinted from Susan Lee, Michael Moskowitz, and Jane Pinelis, *Quantifying Improbability: An Analysis of the Lloyd’s of London Business Blackout Cyber Attack Scenario*, National Security Report NSAD-R-18-027 (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2018).





## Summary

The US Congress has opened the door to novel strategies for defending the country's electric grid. In the Fixing America's Surface Transportation (FAST) Act, which amended the Federal Power Act (FPA) in December 2015, Congress granted the secretary of energy vast new authorities to use when the president declares a grid security emergency. Most important, the secretary can issue emergency orders to power companies to protect and restore grid reliability when attacks on their systems are "imminent" or under way.<sup>1</sup> The FPA is silent, however, on what the secretary might require companies to do and how such orders can bolster their emergency operations.

The onset of an attack would be the worst possible time to develop emergency orders. Instead, before adversaries strike, power companies and government officials should partner to draft basic "template" orders to defend the grid. They could then adjust such orders to fit the specific circumstances of an attack. Developing emergency orders in advance would also help grid owners and operators create detailed, company-specific contingency plans to effectively implement them. Companies could then exercise their contingency plans to build preparedness for response operations and contribute to national security in unprecedented ways.

This report is structured to help the electricity subsector and Department of Energy (DOE) develop emergency orders to defend the grid against potentially catastrophic cyber and physical attacks. The report highlights the phases that grid security emergencies are likely to entail. It analyzes the requirements that emergency orders will need to meet for each phase, and how orders can supplement existing utility plans and capabilities to fill gaps in grid resilience. The report also examines how emergency orders can strengthen deterrence against grid attacks and help defeat adversaries if deterrence fails.

The president must declare a grid security emergency before the secretary of energy can issue emergency orders. However, the FPA offers only broad and potentially ambiguous criteria for making that determination, especially for attacks that are imminent. Such ambiguity is useful; the president should retain the flexibility to declare grid security emergencies in a wide range of circumstances. Nevertheless, policy makers may find it useful to establish more detailed criteria to support their internal deliberations. This report proposes options for them to consider, including criteria derived from the electric industry's requirements to preserve "adequate levels of reliability" against cascading blackouts and other multistate grid disruptions. The report also examines how industry and government agencies can refine their information sharing mechanisms to support the emergency declaration process.

Once the president makes such a declaration, grid security emergencies may roll out in three phases, each of which provides the basis for developing a distinct set of template emergency orders. Figure S-1 illustrates these phases. The first will occur if the president determines that an attack is imminent. A well-established basis already exists for developing preattack emergency orders. When hurricanes or other severe storms are closing in on electric utilities, those utilities can implement *conservative operations* to strengthen their preparedness for potential disruptions. Such operations might include staffing up emergency operations centers, prepositioning recovery personnel and supplies, increasing available generation to help manage grid instabilities, and taking other precautionary measures. A key advantage of many of these options is that utilities can carry them

---

<sup>1</sup> Fixing America's Surface Transportation Act, Public Law 114-94.

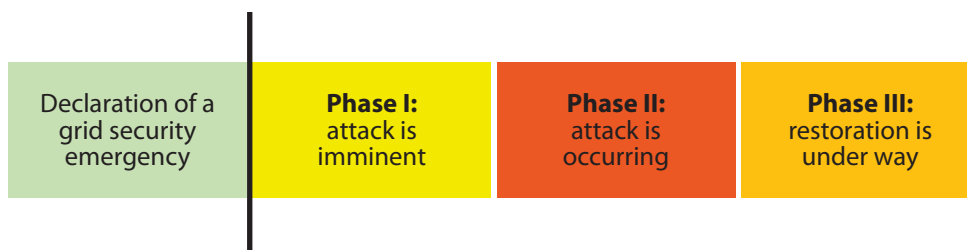


Figure S-1. Grid Security Emergency Phases

out without disrupting normal service; if the hurricane veers back to sea, utilities will have no regrets about having implemented them.

Power companies should help DOE develop equivalent “no-regrets” conservative operations to protect the grid against imminent cyber and physical attacks. A growing number of utilities are already adapting their existing plans for conservative operations to counter physical and cyber risks. These initiatives provide a strong foundation for developing emergency orders that will leverage best practices and help ensure that utilities will implement them on a consistent, nationwide basis. Moreover, because many of these conservative operations will inflict little or no disruption on normal grid service, they are ideal for protecting the grid when attacks are increasingly probable but not certain to occur. DOE and industry should consider prioritizing their development, both for the near-term resilience benefits they would provide and as a means to refine collaborative mechanisms for use in more challenging development efforts.

The next phase of grid security emergencies will occur when attacks are under way. Emergency orders for this phase can help utilities prevent power failures from cascading across the United States and prioritize the sustainment of electric service for military bases and facilities essential for public health (e.g., major regional hospitals and metropolitan water systems). As with conservative operations, existing electric industry plans and capabilities provide a strong basis for developing such emergency orders. For example, when severe damage to grid infrastructure leaves utilities with inadequate power to serve all their customers, they can shed load (i.e., temporarily halt service to customers) to prevent cascading outages. Orders for equivalent *extraordinary measures* could provide useful arrows in the quiver in grid security emergencies.

The final phase of grid security emergencies will commence as utilities begin restoring service to areas without power. Attacks that damage or destroy large numbers of high-voltage transformers and other difficult-to-replace grid components could create outages that darken major portions of the United States for many weeks, or even months. Power companies and DOE already have initiatives under way to meet this challenge. They should also collaborate to develop emergency orders to *support restoration*, which could facilitate the movement of replacement transformers and assist utilities in other strategically vital ways.

These grid security emergency phases could overlap. In particular, once power companies begin restoring power, adversaries may launch follow-on attacks that necessitate continued load shedding and other extraordinary measures to protect grid reliability. At the outset of an emergency, utilities should prepare to receive and implement orders across all emergency phases in an integrated way.

DOE and its industry partners should also design emergency orders to fill underlying gaps in preparedness for cyber and physical attacks. Power companies already have extensive plans and capabilities to protect and restore grid reliability against these threats, in part because mandatory reliability standards require them to do so. Grid owners and operators are also spring-loaded to employ emergency measures the moment they are

needed. Indeed, the North American Reliability Corporation can fine most major US power companies if they fail to implement emergency actions to protect grid reliability.<sup>2</sup> This robust industry preparedness begs the question: what added value can DOE emergency orders provide?

The most obvious benefit lies in the FPA's provisions for regulatory waivers and cost recovery. When grid owners and operators carry out emergency orders, they may have to violate environmental standards and other regulatory requirements. The FPA now protects entities from being punished for such violations if they occur while complying with emergency orders. The act also provides for the recovery of costs that companies will incur in implementing emergency orders. This report examines how further waiver and cost-recovery measures could reinforce preparedness for grid security emergencies.

Emergency orders can also help support national security in new and far-reaching ways. Russia, China, and other potential adversaries will not strike the grid simply to create power outages. They will do so to achieve broader political and military objectives. For example, if the United States and its allies become engaged in a severe regional crisis, adversaries may seek to cripple the flow of power to US defense installations responsible for deploying forces to the region, as well as to ports and other civilian infrastructure that supports force projection. Emergency orders can be designed to help deter—and, if necessary, defeat—such attacks. This report proposes specific options to do so, in support of the *National Security Strategy of the United States of America* and other sources of US policy guidance.

Some of these options will require harsh and politically contentious decisions on allocating power if adversaries severely disrupt the grid. Emergency orders for prioritized load shedding provide a case in point. To help deter attacks, grid owners and operators need the ability to sustain service to critical defense installations, including those responsible for conducting response operations against (and imposing costs on) potential attackers for however long a conflict may last. The ability to protect power flows to hospitals and other facilities vital for public health and safety will be valuable as well. However, if adversaries disrupt sufficient grid generation and transmission assets, sustaining reliable service to these installations may require utilities to curtail service to other customers. Government officials—and, ultimately, the president—should make such decisions and provide political top cover and liability protections for power companies that implement them.

Grid security emergencies will also create unprecedented challenges for government and industry to communicate with the American people. The public declaration of a grid security emergency will be almost certain to spark a media frenzy and a flood of ill-informed speculation. Against a backdrop of fear and uncertainty, adversaries may use social media and other means to spread further disinformation and incite public panic as part of their attacks. Adversaries may also disrupt the phone and internet-based communications systems utilities typically use to coordinate with each other and with DOE. These challenges go far beyond those created by hurricanes or other natural disasters. Industry and government partners should build on their existing array of coordination mechanisms and communications playbooks to prepare for grid security emergencies, and they should make doing so a core component of the emergency order development process.

DOE and its industry and government partners will need to conduct intensive follow-on work to finalize the development of emergency orders and build utility-specific contingency plans to implement the orders in ways that account for accelerating structural changes in the electricity subsector. Their collaborative efforts will

---

<sup>2</sup> Bulk power system entities, including generation and high-voltage transmission companies, are subject to NERC's mandatory reliability standards and emergency orders under the FPA. For an analysis of applicability issues, see pages 5–10.

require significant industry and DOE resources at a time of flat demand for electricity and increasing financial pressure on many power companies.

Nevertheless, as utilities and DOE tackle the immediate challenges of developing emergency orders, they should also explore broader opportunities to build preparedness for grid security emergencies. One such opportunity lies in integrating the use of emergency orders with other federal authorities. The secretary of energy can issue grid security emergency orders only to power companies. Increasingly, however, power generation depends on the flow of natural gas. Communications systems and other infrastructure sectors will also play critical roles in supporting power restoration. The secretary of energy and other federal leaders have additional authorities beyond section 215A of the FPA that can strengthen cross-sector resilience for grid security emergencies. However, achieving these benefits will require private and public sector leaders to preplan and exercise the coordinated use of these authorities, and to develop “whole-of-government” strategies to support infrastructure owners and operators.

Coordination with Canada could be valuable as well. The electric grids of the United States and Canada are deeply interconnected, and adversary-induced failures in one nation may rapidly cascade into the other. The secretary of energy does not have the authority to issue emergency orders to power companies in Canada (or in any other nation). Yet, significant opportunities exist to build on current reliability protections and emergency coordination mechanisms between US and Canadian utilities. The United States could also develop collaborative plans with Mexico as well as US allies in Europe and Asia.

In addition, DOE and its partners should explore further opportunities to help deter cyber attacks and defeat US adversaries if deterrence fails. The US *National Security Strategy* emphasizes that the United States needs to convince adversaries not only that they will suffer costly consequences if they attack but also that attacking will not accomplish the objectives they seek—in other words, achieve deterrence by denial. Yet, leading scholars of deterrence argue that deterrence by denial will be extraordinarily difficult to establish in cyberspace. Emergency orders and implementation plans can help meet these challenges by strengthening grid resilience in novel ways. Government agencies should also consider developing broader doctrine to “play defense” if cyberwarfare breaks out, and coordinate grid security emergency operations at home with measures to suppress adversary attacks at their source.

The foundational importance of the electric grid makes it a prime target for attack. As secretary of energy Richard Perry emphasizes, “America’s greatness depends on a reliable, resilient electric grid” that can power the economy, support national defense, and provide for the necessities of modern life.<sup>1</sup> To prevent adversaries from exploiting the United States’ dependence on the grid, the Department of Energy (DOE) and its industry partners should jointly develop emergency orders under the Federal Power Act (FPA) to help deter—and, if necessary, defeat—attacks on the grid.<sup>2</sup>

The FPA provides only the starting point to launch this collaborative effort. On December 4, 2015, when Congress adopted the Fixing America’s Surface Transportation (FAST) Act amendments to the FPA, it greatly expanded the secretary of energy’s authority to issue emergency orders to grid owners and operators. Under section 215A of the act, “the Secretary may, with or without notice, hearing, or report, issue such orders of emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability” of critical electric infrastructure in a grid security emergency.<sup>3</sup> Before the secretary can issue those orders, the president

must first declare a grid security emergency when attacks on the grid are imminent or under way.<sup>4</sup>

However, legislators provided scant guidance on what the secretary might order power companies to do. DOE and its partners in the electricity subsector are now assessing which specific types of emergency orders would be most helpful to protect and restore grid reliability against emerging threats. This report supports their work by examining possible emergency orders and analyzing broader opportunities to strengthen resilience for grid security emergencies.

## Developing Emergency Orders under the FPA: Collaborative Opportunities, Fundamental Goals, and Overarching Design Requirements

The secretary of energy’s new authorities are so vast that they entail a potential risk: issuing ill-conceived, poorly coordinated emergency orders could hurt rather than help power company operations. As President Reagan famously noted, “the nine most terrifying words in the English language are ‘I’m from the government and I’m here to help.’”<sup>5</sup> Emergency orders that are technically impossible for electric companies to implement, or that inadvertently jeopardize grid reliability, could disrupt grid defense and exacerbate the effects of enemy attacks.

DOE is already taking steps to minimize such risks. Especially valuable, the department has incorporated industry recommendations on the process by which the secretary should issue emergency orders to utilities, and—“if practicable”—consult with industry before those orders are issued.<sup>6</sup> The next collaborative step should be to include power companies in

<sup>1</sup> Perry, letter to the FERC.

<sup>2</sup> The 2015 FAST Act amendments to the FPA provide the authority to undertake these efforts. Prior to 2015, section 202(c) of the FPA already authorized the secretary of energy to issue emergency orders to order “temporary connections of facilities, and generation, delivery, interchange, or transmission of electricity as the Secretary determines will best meet the emergency and serve the public interest.” That provision also specified that the secretary could exercise such powers “during the continuance of a war in which the United States is engaged or when an emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy, or of facilities for the generation or transmission of electric energy, or of the fuel or water for generating facilities, or other causes.” See “DOE’s Use of Federal Power Act Emergency Authority,” DOE. The 2015 FAST Act amendments to the FPA gave the secretary further powers (mostly incorporated in section 215A of the act), which are the primary focus of this report.

<sup>3</sup> 16 U.S.C. § 824o, (b)(1).

<sup>4</sup> The analysis that follows examines the definition of such emergencies in the FPA and potential thresholds for declaring them.

<sup>5</sup> Reagan, “President’s News Conference.”

<sup>6</sup> DOE, “RIN 1901–AB40,” 1176; EEI, “Comments”; and Paradise et al., “ISO-RTO Council Comments.”



designing template emergency orders. Grid owners and operators have unequaled knowledge of their own infrastructure and operating procedures and extensive experience in employing emergency measures to protect and restore grid reliability.<sup>7</sup> They are well positioned to assess how complying with emergency orders could adversely impact grid operations, violate environmental regulations, or incur extraordinary expenses—and how FPA provisions for waivers and cost recovery can help address these problems. Most importantly, grid owners and operators can help determine which types of orders would be most useful to help defend their systems and effectively supplement the emergency measures utilities would already be taking on their own. Utilities will also play a critical role in building company-specific plans to implement emergency orders, exercising those plans, and identifying remaining gaps to fill.

Strategic guidance from DOE and other government departments will be just as critical for designing emergency orders. Federal leadership will be essential to ensure that emergency orders help achieve overarching US security goals, both to deter attacks on the United States and to defeat adversaries if deterrence fails. Framing emergency orders to support execution of the *National Security Strategy of the United States of America* (December 2017) will be especially important to counter threats from Russia, China, and other potential adversaries.<sup>8</sup> Government officials can also shape emergency orders and supporting initiatives to help implement US cyber resilience strategies, including the *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

(May 2017) and DOE's *Multiyear Plan for Energy Sector Cybersecurity* (March 2018).<sup>9</sup>

In addition, DOE will play a critical role in coordinating industry and government operations during grid security emergencies. The same congressional amendments that granted the secretary expansive new emergency authorities also specified that DOE shall be the federal government's "lead sector-specific agency for cybersecurity for the energy sector." As such, the secretary is responsible for collaborating with grid owners and operators, regulators, and other government agencies to help mitigate incidents and provide broader support to the energy sector.<sup>10</sup>

Federal incident response operational plans provide a broader framework for building these collaborative mechanisms. Presidential Policy Directive 41, *United States Cyber Incident Coordination* (July 2016), the *National Cyber Incident Response Plan* (December 2016), and the *National Response Framework* (June 2016) offer particularly useful guidance for building grid-specific coordination mechanisms.<sup>11</sup> DOE is also strengthening its own internal mechanisms and organizational structure to manage cyber incidents.<sup>12</sup> These changes further position the department to effectively collaborate with industry in developing and executing emergency orders.

<sup>9</sup> Trump, *Executive Order on Strengthening Cybersecurity*; and DOE, *Multiyear Plan*. See also Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity*; and DHS, *Cybersecurity Strategy*.

<sup>10</sup> Fixing America's Surface Transportation Act, Public Law 114-94, 1779 (hereafter cited as FAST Act).

<sup>11</sup> Obama, *United States Cyber Incident Coordination*; DHS, *National Cyber Incident Response Plan*; and DHS, *National Response Framework*.

<sup>12</sup> DOE, *Multiyear Plan*, 28. DOE has also established the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to "enable more coordinated preparedness and response to natural and man-made threats." See "Secretary of Energy Forms New Office," DOE.

<sup>7</sup> FERC and NERC, *Restoration and Recovery Plans*; FERC and NERC, *Planning Restoration Absent SCADA or EMS (PRASE)*; and FERC and NERC, *Recommended Study: Blackstart Resources Availability (BRAv)*. Additional BPS plans, exercises, and mandatory reliability standards are addressed in subsequent portions of the report.

<sup>8</sup> White House, *National Security Strategy*.



## Drafting Template Emergency Orders before Attacks Occur

The FPA specifies that before issuing emergency orders “the Secretary shall, to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action,” consult with appropriate power companies and other grid resilience stakeholders.<sup>13</sup> But opportunities for such consultations may be sharply limited. Adversaries may strike the grid with little or no warning. Moreover, when attacks are imminent or under way, rapidly issuing emergency orders may be crucial to help prevent cascading failures and other widespread disruptions. This imperative for speed could make consultations impractical.

To enable collaboration and minimize the risk that DOE will have to create orders amid the chaos of an attack, grid owners and operators should help DOE develop orders well before attacks occur. Bruce J. Walker, assistant secretary of energy for electricity delivery and energy reliability, stated in March 2018: “In preparation for any future grid security emergency, it is critical that we continue working with our industry, Federal, and state partners now to further shape the types of orders that may be executed under the Secretary’s authority, while also clarifying how we communicate and coordinate the operational implementation of these orders.”<sup>14</sup> Power companies and other electricity subsector organizations have also emphasized the need for industry and the government to jointly develop orders before adversaries strike.<sup>15</sup>

Such collaborative efforts should initially focus on creating *template orders*: orders that lay out the

basic types of actions that the secretary might direct grid owners and operators to conduct. Template orders should occupy the middle ground between including too few operational requirements versus too many. It would be a waste of the FAST Act amendments’ potential value for the secretary to issue general orders to “protect and restore the reliability of the grid.” Vague, overly broad directives cannot provide an adequate basis for utilities to develop system-specific plans to implement them. Instead, DOE and industry should build on the options that many utilities already have for specific emergency operations, from easy-to-implement orders such as requirements for “maximum generation” and increased reserve margins to more aggressive, far-reaching measures.<sup>16</sup> A key objective for such development efforts: provide a menu of agreed-upon options from which the secretary can choose as circumstances require, supported as much as possible by consultations with industry.

Developing emergency orders before attacks occur can help ensure that, as a minimalist goal, such orders will “do no harm.” By participating in the order design process, power companies can shape orders to account for system-specific engineering constraints and requirements for emergency operations. This industry input will be especially important because DOE has the authority to punish utilities for failing to comply with emergency orders, even if they are poorly designed. DOE’s grid security emergency rule specifies that “in accordance with available enforcement authorities, the secretary may take or seek enforcement action against any entity subject to an emergency order who fails to comply with the terms of that emergency order.”<sup>17</sup> If

<sup>13</sup> This includes the North American Electric Reliability Corporation (NERC) and its Electricity Information Sharing and Analysis Center (E-ISAC). 16 U.S.C. § 824o–1. See also the notice of proposed rulemaking and request for comment (DOE, “RIN 1901–AB40”).

<sup>14</sup> Walker, *Written Testimony*.

<sup>15</sup> See Joint Commenters, “Comments; and NASEO, “Comments.”

<sup>16</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See PJM, *PJM Manual* 13, 35. Reserve margins consist of generation capacity over and above projected peak demand. Increasing reserve margins can help “maintain reliable operation while meeting . . . unexpected outages of existing capacity.” See “M-1 Reserve Margin,” NERC.

<sup>17</sup> DOE, “RIN 1901–AB40,” 1182.

power companies find that an order is impossible to implement or is otherwise objectionable, they can ask DOE to reconsider it.<sup>18</sup> But adjudicating individual emergency orders amid a grid security emergency could delay time-critical actions. Instead, DOE should include industry in developing emergency orders from the start and resolve utility concerns before adversaries strike.

Preplanning to coordinate industry and government emergency operations will also be valuable. Power companies are already poised to take immediate emergency actions to protect grid reliability as circumstances require, regardless of whether the secretary issues emergency orders. It will be helpful to understand in advance how DOE can best align the issuance of such orders with industry-initiated actions. Once attacks are under way, preplanning for operational coordination will become still more important, especially if adversaries continue striking the grid and its supporting communications systems after their initial salvo.

If attacks do occur, Russia, China, or other potential adversaries will use country-specific tactics, techniques, and procedures to disrupt US infrastructure. Defending against those attacks will require tactical and operational responses that are similarly tailored to specific adversaries. Over time, it may be possible to develop (and protect adversaries from accessing) emergency orders that account for these individualized defensive requirements. US leaders should also consider building country-specific contingency plans that integrate infrastructure defense operations with measures abroad to halt or disrupt attacks on the grid, in ways that are mutually supportive rather than ad hoc and uncoordinated. The conclusion of this report examines opportunities to do so.

Initially, however, industry and government should partner to develop template orders that could be used against a range of adversaries. These orders

should also be sufficiently broad to allow utilities to implement the required actions in ways that match their own specific systems and service areas. Every utility depends on a unique configuration of generation assets, high-voltage transmission lines, and other grid infrastructure. Utilities also differ in terms of the military bases, regional hospitals, and other critical customers that may need prioritized service during emergencies. Establishing template orders will give power companies the basis they need to build detailed, system-specific implementation plans, rather than attempting to include that level of detail in the orders themselves.

Developing template orders before adversaries strike will offer other advantages as well. Once such orders are in place, power companies and their government partners will be able to design exercises that test and strengthen their abilities to execute the orders, uncover hidden gaps in preparedness, and identify opportunities to improve order design and execution. Training programs to prepare employees to carry out utility-specific implementation plans should also get under way as soon as possible. On a larger scale, utilities will also be able to exercise the implementation of template emergency orders within the framework of the Cyber Mutual Assistance (CMA) Program. This program enables over 140 utilities in the United States and Canada to address potential challenges in allocating scarce cyber response capabilities, assist each other when adversaries strike, and coordinate outreach to state National Guard organizations and other potential partners.<sup>19</sup> Exercises can help determine how best to align the issuance and implementation of emergency orders with these growing capabilities for mutual support.

Having template orders in hand could also facilitate internal government decision-making in grid security emergencies. While the secretary of energy has the sole authority to issue emergency orders, the secretary may request input from senior DOE staffers

<sup>18</sup> DOE, "RIN 1901-AB40," 1181-1182.

<sup>19</sup> "ESCC's Cyber Mutual Assistance Program," ESCC.

on which orders will be most useful against specific types of attacks. The secretary may also need to brief the president and the National Security Council on proposed orders and their potential benefits. By developing orders and clarifying their respective advantages before adversaries strike, DOE and industry partners can facilitate such deliberations.

Over the longer term, industry and government leaders might structure their collaboration to provide additional security benefits. To meet the technical and organizational complexities of preparing for advanced biological threats, for example, the use of common planning cases offers unique opportunities to strengthen public-private and interagency coordination.<sup>20</sup> Building planning cases for the issuance and implementation of FPA emergency orders could offer equivalent benefits, especially if conducted within the robust mechanisms for government-industry collaboration already established by the Electricity Subsector Coordinating Council (ESCC).

However, to develop template emergency orders and contingency plans to implement them, power companies will need to conduct extensive operational and engineering studies and use enhanced modeling to understand the potential impact of such orders. The FAST Act amendments to the FPA provide no funding for such development efforts. Moreover, DOE and power companies are only the most obvious participants in the order design process. A wide array of other grid resilience and incident management stakeholders may also need to assist that process—including critical ones not mentioned in the FPA. Determining which specific public and private sector organizations should help shape template orders constitutes a critical first step in preparing for grid security emergencies.

## Participants in Drafting and Implementing Emergency Orders: The Bulk Power System and the Broader Electricity Subsector

An initial task in developing emergency orders will be to determine which components of the electricity subsector should participate in that effort. DOE defines the electricity subsector as the “portion of the energy sector [that] includes the generation, transmission, distribution, and marketing of electricity.”<sup>21</sup> The most obvious candidates for inclusion are the power companies that are subject to emergency orders. The FAST Act amendments to the FPA specify which components fall into that category. Chief among them are “any owner, use or operator of critical electric infrastructure or of defense critical electric infrastructure within the United States.”<sup>22</sup> The FPA also includes criteria to identify this infrastructure. Critical electric infrastructure comprises grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters.”<sup>23</sup> Defense critical electric infrastructure consists of grid components that serve facilities “critical to the defense of the United States” and that are vulnerable to the disruption of grid-provided power.<sup>24</sup>

However, Congress also narrowed the definition of critical electric infrastructure in a significant way. The FPA states that such infrastructure only includes assets that compose the bulk power system (BPS). BPS assets are those “facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generation

<sup>20</sup> Danzig, *Catastrophic Bioterrorism*, 5–7; and Blue Ribbon Study Panel, *National Blueprint*, 13, 42–44.

<sup>21</sup> DOE, *Electricity Subsector Cybersecurity Capability Maturity Model*, 5.

<sup>22</sup> 16 U.S.C. § 824o–1, (b)(4)(c).

<sup>23</sup> 16 U.S.C. § 824o–1, (a)(2).

<sup>24</sup> 16 U.S.C. § 824o–1, (a)(4).

facilities needed to maintain transmission system reliability.”<sup>25</sup> These BPS generation and transmission assets provide synchronized power within the three interconnections that serve the entire United States and parts of Mexico and Canada.<sup>26</sup>

As defined by the FPA, the BPS does not include infrastructure used for the local distribution of electric power.<sup>27</sup> That limitation creates a potential problem for executing emergency orders. Local distribution systems often provide the “last mile” of connectivity between transmission systems and military bases and other critical customers. As DOE and industry create template emergency orders and execution plans, it will be essential to integrate local distribution providers into that development process.

However, before examining these distribution-level issues, it will first be helpful to clarify the components of the BPS that are explicitly subject to emergency orders under the FPA (and are therefore key partners for DOE in designing them). The FPA states that the secretary of energy may issue emergency orders to the following the BPS “entities:”<sup>28</sup>

**The Electric Reliability Organization.** After blackouts cascaded across major portions of the United States in August 2003, Congress authorized the Federal Energy Regulatory Commission (FERC) to certify an electric reliability organization to develop and enforce, subject to FERC approval, mandatory

electric reliability standards for all users, owners, and operators of the US BPS.<sup>29</sup> FERC certified the North American Electric Reliability Council (NERC) as the first-ever electric reliability organization in July 2006. Renamed the North American Electric Reliability Corporation in 2007, it has served in that role since.<sup>30</sup> NERC’s mission is to ensure the reliability and security of the BPS in North America. As such, NERC is uniquely positioned to help DOE develop emergency orders, especially for attacks that could create cascading blackouts or other multistate disruptions of critical electric infrastructure.

NERC also operates the Electricity Information Sharing and Analysis Center (E-ISAC), which plays a leading role for the electricity subsector in establishing situational awareness, incident management and coordination, and communication capabilities.<sup>31</sup> E-ISAC capabilities for conducting threat assessments, gathering incident data, and sharing information among utilities and their government partners will be vital for responding to grid security emergencies.

**Regional entities responsible for enforcing reliability standards for the BPS.**<sup>32</sup> NERC has delegated certain authorities to eight regional entities to monitor and enforce compliance with reliability standards.<sup>33</sup> While regional entities play major oversight roles, they do not directly operate the physical grid and would not, on their own, be positioned to execute emergency orders. However, they could help utilities and DOE and preplan for

<sup>25</sup> 16 U.S.C. § 824o, (a)(1).

<sup>26</sup> Interconnections are defined as the “geographic area in which the operation of Bulk Power System components is synchronized such that the failure of one or more of such components may adversely affect the ability of the operators of other components within the system to maintain Reliable Operation of the Facilities within their control.” North America includes four major electric system networks: the Eastern, Western, Quebec, and Energy Reliability Corporation of Texas (ERCOT) interconnections. See NERC, *Glossary*.

<sup>27</sup> The BPS specifically excludes local distribution facilities, though it does not provide criteria to identify “local” distribution. See 16 U.S.C. § 824o, (a).

<sup>28</sup> 16 U.S.C. § 824o–1, (b)(4).

<sup>29</sup> Energy Policy Act of 2005, Public Law 109-58. This does not include Alaska or Hawaii.

<sup>30</sup> NERC, *History*. For more information on NERC, see “About NERC,” NERC.

<sup>31</sup> “Electricity Information Sharing and Analysis Center,” NERC.

<sup>32</sup> DOE, “RIN 1901–AB40,” 1177. See also 16 U.S.C. § 824o, (a)(7).

<sup>33</sup> “Key Players,” NERC. In July 2017, however, one regional entity announced its intention to dissolve. FERC has approved the dissolution, effective July 2018. See FERC, *Order Granting Approvals* (163 FERC ¶ 61,094).



issuing regulatory waivers to BPS grid operators as they comply with emergency orders.

**Owners, users, and operators of critical electric infrastructure or defense critical electric infrastructure within the United States.**<sup>34</sup> Companies that own and operate generation and transmission assets will be among the most likely recipients of emergency orders and should play a critical role in designing them. Reliability coordinators will be similarly important. Reliability coordinators are the entities that constitute “the highest level of authority” for the reliable operation of the bulk electric system (BES).<sup>35</sup> They are also responsible for maintaining a “wide-area view” of the BES and have the operating tools, processes and procedures, and authority to prevent or mitigate emergency operating situations. As such, reliability coordinators will be critical for designing, receiving, and implementing emergency orders to counter attacks that individual BPS owners and operators may not have the ability to defeat. Seven regional transmission organizations and independent system operators, most of which are registered as reliability coordinators, also help operate and ensure the reliability of the BES in many regions of the United States.<sup>36</sup> Accordingly, regional

transmission organizations and independent system operators will be essential to the design and execution of emergency orders.

### **Local Distribution Providers and Other Grid Resilience Stakeholders**

The 2015 FAST Act amendments to the FPA do not explicitly address the possible roles of local distribution systems in grid security emergencies. However, local distribution infrastructure is critical for overall resilience against cyber and physical attacks. Even if emergency orders help defeat attacks on BPS assets, adversaries may still be able to achieve catastrophic effects by striking multiple local distribution systems and thereby interrupting the flow of power from transmission systems to military bases, hospitals, and other end users. Local distribution systems may also need to help implement emergency orders issued to BPS entities. For example, if the secretary orders transmission systems to protect reliability by shedding load, yet at the same time sustain the flow of power to city water systems and other priority customers, local distribution infrastructure will be essential to conduct such prioritized load shedding. Holistic preparedness for grid security emergencies therefore requires engagement with local distribution systems.

These systems will also have strong incentives to participate in the emergency order planning process. Just as BPS entities rely on local distribution utilities, these utilities rely on generation, transmission, and higher-voltage distribution entities to serve end users. Local systems will also share the commitment of BPS entities to protect and rapidly restore service to defense installations and other critical customers. By integrating local distribution utilities

---

<sup>34</sup> The analysis that follows later in this section examines the definition of “users” of critical electric infrastructure and defense critical electric infrastructure.

<sup>35</sup> While the BPS broadly encompasses all generation and transmission assets necessary to operate a reliable, interconnected grid, the BES is a subset of the BPS that includes, with some exclusions, all transmission and real and reactive power sources at one hundred kilovolts or higher. As with the BPS definition, the BES definition excludes local distribution providers. For these definitions, as well as the definition of reliability coordinators, see NERC, *Glossary*. Consistent with the FPA and the authorities it provides for handling grid security emergencies, this report focuses on the application of emergency orders to BPS entities specifically.

<sup>36</sup> There are ten regional transmission organizations and independent system operators under NERC’s purview, though three operate exclusively in Canada. Regional transmission organizations and independent system operators are independent membership-based nonprofit organizations that ensure reliability and optimize supply and demand bids for wholesale electric power. In other parts of the country, electricity systems are

---

operated by individual utilities or utility holding companies. See “About 60% of U.S. Electric Power Supply Managed by RTOs,” US Energy Information Administration. Six of the seven regional transmission organizations/independent system operators operating in the US are also current reliability coordinators. See “Reliability Coordinators,” NERC.

into emergency order planning, these utilities will be able to participate in shaping template orders and implementation plans to help achieve their reliability goals when adversaries strike. Moreover, to the extent that local distribution companies may be subject to emergency orders, they may also benefit from the FPA's liability protections and cost-recovery provisions for actions taken to execute those orders.

DOE and other stakeholders may determine that the FPA already gives the secretary adequate authority to issue emergency orders to local distribution companies. The act states that emergency orders may apply to "any owner, user, or operator of critical electric infrastructure or defense critical electric infrastructure" within the United States.<sup>37</sup> The act, however, does not further define owners, users, and operators. Pending clarification of these terms by DOE or through judicial review, it might be reasonable to assume that local distribution utilities could be subject to emergency orders if they serve critical facilities under the act.

Regardless of whether the secretary can issue orders to local distribution utilities, BPS entities should include them in building the contingency plans to implement emergency orders. This preplanning will be essential to strengthen comprehensive, end-to-end protection of grid reliability against attacks.

Many companies that own transmission assets also own distribution infrastructure. These utilities will find it relatively easy to include distribution assets in their emergency planning. Integrated response plans will also be necessary for BPS entities that own both generation and transmission assets. Such planning will be easiest for "vertically integrated" utilities that own and operate assets for all three functions. However, many municipally owned electric utilities and rural electric cooperatives (including those that serve critical and defense critical electric infrastructure) are not part of vertically integrated companies. In US regions where generation, transmission,

and distribution systems exist as separate entities, additional engagement initiatives will be essential to implement emergency orders and sustain power to essential facilities.

Including state regulators and other state officials in these integrative efforts could offer additional benefits. State public utility commissions have primary regulatory jurisdiction over distribution systems.<sup>38</sup> The National Association of Regulatory Utility Commissioners, which represents state regulators nationwide, has focused growing attention on the need for prudent utility investments in cyber and physical resilience.<sup>39</sup> Commissioners in New Jersey and other states are also leading regulatory initiatives to bolster cyber resilience in their respective jurisdictions.<sup>40</sup> Emergency managers and National Guard leaders in a growing number of states are also building new mechanisms to coordinate with utilities in responding to cyber attacks. Adding such additional partners to help design emergency orders and plan for their implementation would complicate an already far-reaching engagement process. Nevertheless, incorporating perspectives from state commissioners and other officials would help advance comprehensive state-level preparedness for grid security emergencies.

### Additional Partners for Engagement

DOE and power companies will need to collaborate with a wider array of partners to develop and execute some potentially useful emergency orders, especially to support grid restoration. The final rule

<sup>37</sup> 16 U.S.C. § 824o, (b)(4)(a).

<sup>38</sup> The US Constitution, in most cases, allows federal regulation of private economic activity only for interstate commerce. While this applies to high-voltage, interstate electricity transmission, it does not apply to lower-voltage retail distribution. See Lazar, *Electricity Regulation in the US*, 15.

<sup>39</sup> See NARUC, *Cybersecurity*; and NARUC, *Resolution on Physical Security*.

<sup>40</sup> State of New Jersey Board of Public Utilities, *In the Matter of Utility Cyber Security Program Requirements* (Docket No. AO16030196).



on *Grid Security Emergency Orders: Procedures for Issuance* (hereinafter referred to as the grid security emergency rule) notes: “Historically, the Department has collaborated with other Federal agencies in an energy emergency to obtain waivers or special permits” to expedite the restoration of power.<sup>41</sup> This includes traditional partners such as the Department of Homeland Security (DHS) and the Department of Defense (DOD). Still broader collaboration with government and private sector partners may be valuable for implementing emergency orders to restore grid reliability.

Transformer replacement operations offer a prime example. If adversaries destroy large power transformers at substations across the United States, and these attacks cut off power to critical military bases, the secretary might order industry to prioritize the replacement of large power transformers at substations of greatest importance to national security. The electric power industry has established an extensive Spare Transformer Equipment Program to provide for such replacements.<sup>42</sup> New industry-led organizations such as Grid Assurance,<sup>43</sup> as well as programs such as the Regional Equipment Sharing for Transmission Outage Restoration (RESTORE) initiative, are further expanding the industry’s capacity to replace transformers and other equipment.<sup>44</sup> These efforts will be essential for preparing for grid security emergencies, especially as industry stocks and securely stores the full range of replacement transformer types and sizes that large-scale physical attacks may require.

However, power companies do not move large power transformers by themselves. They rely on railroad companies, barges, and heavy-haul trucking companies to help do so and have established a

Transformer Transportation Working Group under the ESCC to plan and coordinate transformer movement.<sup>45</sup> Exercises in the Spare Transformer Equipment Program now involve representation from transportation stakeholders. Yet, the FPA does not give the secretary authority to issue orders to transportation companies. In anticipation of orders for replacing transformers, transmission system owners and operators should consider building contingency plans with transportation companies to help execute those orders. Preplanning with the US Department of Transportation (DOT), the Federal Emergency Management Agency (FEMA), and state governments to get contracts, permits, and regulatory waivers to expedite transformer movement will also be useful. In addition, advance coordination with emergency managers at all levels of government would help them mitigate the effects of rotating blackouts or other extraordinary measures on public health and safety.

DOE and the electricity subsector should consider expanding the geographic scope of these discussions as well. In defining the defense critical electric infrastructure that emergency orders can protect, Congress excluded grid assets in Alaska and Hawaii.<sup>46</sup> But both states are home to vital military installations, as are a number of US territories. The secretary also lacks the authority to issue emergency orders to Canadian utilities. Yet, US and Canadian electric systems are deeply integrated, and coordinated efforts to prevent instabilities in grid security emergencies could benefit both nations. Collaborations with NATO allies and other security partners in the face of major adversarial cyber campaigns could be valuable as well. The concluding section of this report examines the potential benefits of expanding grid

<sup>41</sup> DOE, “RIN 1901–AB40,” 1177.

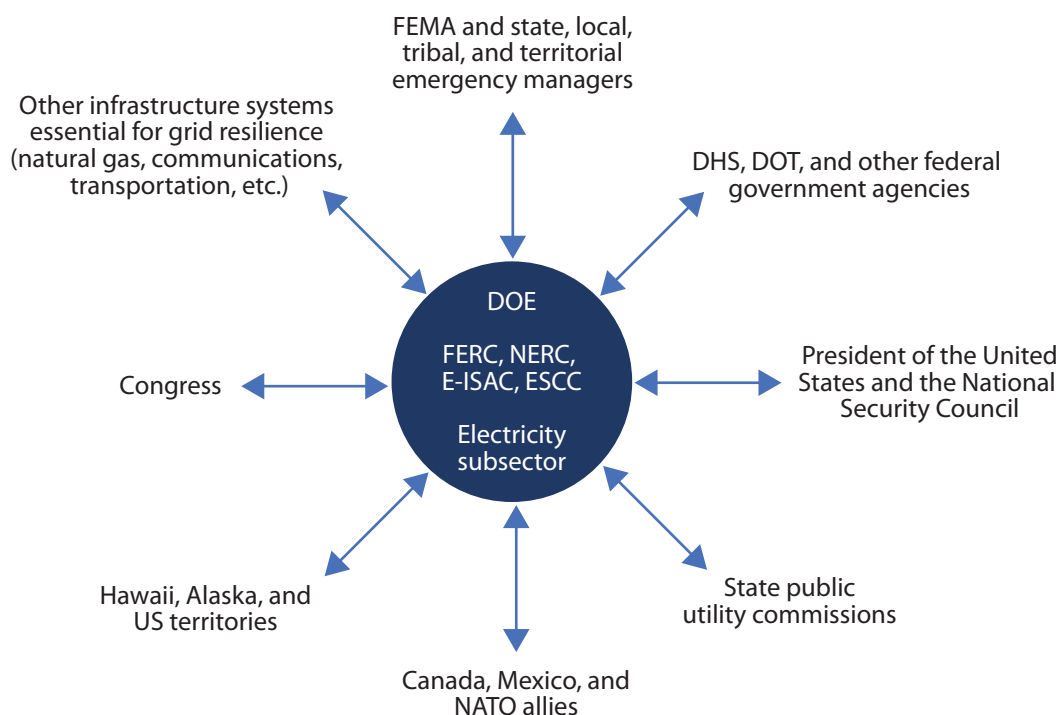
<sup>42</sup> See DOE, *Strategic Transformer Reserve*; and “Spare Transformers,” EEL.

<sup>43</sup> “Transmission Equipment Ready,” Grid Assurance.

<sup>44</sup> FERC, *Order Authorizing Acquisition and Disposition* (163 FERC ¶ 61,005), 10.

<sup>45</sup> DOE, *Strategic Transformer Reserve*, 12.

<sup>46</sup> 16 U.S.C. § 824o–1, (a)(4). The FPA’s section on electric reliability, including the definition of BPS, also excludes entities in Alaska and Hawaii, further constraining the authority of the secretary to issue emergency orders to such entities. See 16 U.S.C. § 824o, (k).



**Figure 1. Stakeholders for Building Grid Security Emergency Resilience**

security emergency coordination within the United States and beyond.

Figure 1 illustrates the array of partners that might help build preparedness for such emergencies. DOE, BPS entities, and the broader electricity subsector comprise the core of the team needed to design, issue, and implement emergency orders. DOE defines the electricity subsector as the “portion of the energy sector [that] includes the generation, transmission, distribution, and marketing of electricity.”<sup>47</sup> This definition comprises the key subsector components represented in the ESCC, to include owners and operators of electric generation, transmission, and distribution assets “from all ownership categories.”<sup>48</sup> As such, the ESCC is ideally suited to coordinate with

DOE in the order development process, together with NERC, the E-ISAC, and other BPS entities and trade associations.

Surrounding these core participants are additional partners that might offer valuable insights for developing orders and coordinating emergency response operations. Some of these partners (including Congress) can also help oversee the implementation of the FPA’s emergency provisions and assess requirements for further statutory changes.

Of course, the full set of potential contributors to emergency preparedness is broader still. For example, vendors who can help utilities replace damaged relays and other equipment could play vital roles. So could law enforcement agencies, cybersecurity contractors, state National Guard organizations, and other sources of expertise and support for power companies. National laboratories and other research and development organizations will also need to sustain their support for improved grid resilience. Over time, comprehensive engagement with all such partners could pay major dividends.

<sup>47</sup> DOE, *Electricity Subsector Cybersecurity Capability Maturity Model*, 5.

<sup>48</sup> In addition to infrastructure owners and operators, ESCC membership includes regional transmission organizations and independent system operators, NERC, the National Infrastructure Advisory Council, and the Canadian Electricity Association. ESCC, *Electricity Sub-Sector Coordinating Council Charter*, 3.

## Goals and Specific Design Requirements for Developing Emergency Orders

The starting point in developing template emergency orders is to identify the objectives, scope, and design requirements that these orders will need to encompass. Key issues analyzed in the sections of the report that follow:

- **Threats, triggers, and thresholds for issuing emergency orders.** Only a limited number of natural and man-made hazards can trigger a grid security emergency.<sup>49</sup> Countering each of those hazards will require threat-specific emergency orders. Hence, the first step for developing such orders will be to examine the threats and attack scenarios on which the design process should focus and clarify the criteria that the president might use to determine that a grid security emergency exists—including when there is an “imminent danger” of an attack.
- **Designing emergency orders for sequential phases of grid security emergencies.** Different types of emergency orders will be needed to protect grid reliability (1) when attacks are imminent, and (2) when attacks are under way. Promising opportunities also exist to develop orders for a third phase of grid security emergency operations: the restoration of grid reliability if adversaries inflict major blackouts on the United States.
- **Incorporating national security policies and priorities into emergency order design.** Adversaries may strike the grid to disrupt the flow of power to defense installations and other facilities essential to national security. Many utilities are already collaborating with defense partners to build redundant power feeds for these facilities and make other targeted

investments in resilience. A growing number of grid owners and operators also plan to prioritize the restoration of power to military bases if blackouts occur. Emergency orders provide a unique opportunity for DOE and its partners to build on such initiatives, and provide more systematic, comprehensive, and effective support to national security.

An initial step to do so is to ensure that emergency orders reflect and help achieve broader federal government strategies to defend critical infrastructure. Most important, the US *National Security Strategy* specifies how the United States will deter attacks on critical systems and—if deterrence fails—how it will defeat the attackers.<sup>50</sup> DOE and its industry partners should design emergency orders to help implement the strategy, as well as meet the specific requirements of the FPA.

Government leaders will need to support this design process with two further steps. First, agencies will need to identify the military bases and other facilities whose electric service will be most important to protect and restore. The FPA provisions and existing industry plans to prioritize the restoration of power will provide a useful starting point. Second, agencies will need to share this data (in carefully protected ways) with power companies so that they can prepare contingency plans to implement emergency orders and help defend the nation.

Emergency orders and implementation plans also offer a basis to clarify how US agencies and private companies will coordinate their operations during cyberwarfare, and build consensus on the private sector’s emerging role in national security. No power company has ever tried to maximize shareholder value by promising to bolster cyber deterrence or help defeat attacks by nations such as Russia or China. Yet, because

---

<sup>49</sup> In addition to being triggered by cyber attacks, grid security emergencies can be triggered by electromagnetic pulse attacks, geomagnetic storms, or direct physical attacks. 16 U.S.C. § 824o–1, (a)(7).

---

<sup>50</sup> White House, *National Security Strategy*, 13.

of the grid's importance to the economy, public health and safety, and national defense, the United States needs a doctrinal framework to coordinate industry and government actions during attacks on the US electric system.<sup>51</sup> Scott Aaronson, Edison Electric Institute's vice president for security and preparedness, notes that "there is not a lot of doctrine around cyber attacks on civilian infrastructure."<sup>52</sup> Building such doctrine and operationalizing public-private partnerships will be crucial for grid security emergency preparedness.

- **Communications.** The declaration of a grid security emergency, much less the spread of adversary-induced blackouts across the United States, will create immense communications challenges for government and industry. The grid security emergency rule describes the consultative process that (if practicable) will occur before the secretary issues emergency orders.<sup>53</sup> However, the grid security emergency rule does not address the risk that adversaries will attack the industry-government communications systems necessary to issue orders, monitor their implementation, and defeat adversaries' attacks.

Building secure, survivable communications will be essential to effectively issuing and implementing emergency orders. However, the FPA provides no requirements or funding to do so. The electricity subsector is currently working with government agencies and telecommunications companies to advance secure communications initiatives. These partners should treat preparedness for grid security emergencies as a special area of focus, including measures to

ensure that grid owners and operators can verify the authenticity of emergency orders.

Government and utility leaders will also need to coordinate what they tell the American people when the secretary issues emergency orders. Some orders that will be valuable for managing severe grid disruptions, including those for prioritized load shedding, could cut off electricity to many thousands of customers. Emergency orders that will have such effects should be accompanied by preplanned communications playbooks to address customer concerns.

Communications playbooks should also account for a further risk: that of information warfare by Russia or other adversaries. Attackers will strike the grid to achieve political benefits, including, potentially, the incitement of public panic and a loss of confidence in US leaders. To promote unity of messaging against such efforts, it will be essential to build on existing subsector playbook development and coordination mechanisms via the ESCC, tailored to support the issuance of emergency orders.

- **Waivers and cost recovery.** Complying with emergency orders could cause companies to violate environmental standards or other rules or regulations. The FPA shields companies carrying out emergency orders from liability for what would otherwise be violations of the act itself, FERC-approved reliability standards, or environmental regulations.<sup>54</sup> However, emergency orders will be easier to implement if they include preplanned waivers of regulations beyond the existing provisions of the FPA, particularly in other sectors on which emergency operations will depend.

<sup>51</sup> For DOD's definition of doctrine and an analysis of its benefits for joint warfighting, see Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*.

<sup>52</sup> Lynch, "How the Russian Government Allegedly Attacks."

<sup>53</sup> DOE, "RIN 1901-AB40," 1181.

<sup>54</sup> These waivers apply unless companies carry out orders and related actions in a "grossly negligent manner." See 16 U.S.C. § 824o-1, (f)(4).



The FPA also directs the establishment of mechanisms so that power companies can recover the substantial costs they may incur in complying with emergency orders.<sup>55</sup> Industry–government dialogue will be essential to clarify reimbursement criteria and associated procedures. Yet, that effort will constitute only part of the broader preplanning needed for the financial turbulence that grid security emergencies could create. This study also examines possible emergency orders that would require investments in grid infrastructure to implement. The FPA does not authorize government spending on such pre-emergency projects. If DOE and its partners decide that investment-dependent orders have sufficient value for grid resilience, these partners (and Congress) should explore government funding options that reflect the national security benefits of such orders, rather than increase the electricity bills paid by private citizens.

- **Opportunities for broader resilience against grid security emergencies.** Power companies and DOE may find it helpful to develop a comprehensive plan to sequence and integrate all of the initiatives outlined above. Such a plan might also account for three additional opportunities for progress: (1) employing additional government authorities to coordinate emergency operations between electric utilities and companies in other infrastructure sectors, including the natural gas providers on which power generation increasingly depends; (2) deepening US partnerships with Canada to help protect the interconnected North American power grid, and exploring opportunities for collaboration with Mexico and other nations; and (3) examining longer-term opportunities to leverage improvements in grid resilience to strengthen cyber deterrence, and assessing the risks and potential benefits of coordinating cyber defense operations at home and abroad.

## Threats, Thresholds, and Consultative Options for Declaring Grid Security Emergencies

The FPA leaves the president substantial latitude to determine whether a grid security emergency exists. That flexibility is valuable and should be retained. Nevertheless, as industry and government partners collaborate to develop emergency orders, they should build consensus on the types of threats that ought to drive and sequence the development process. These partners should also examine possible decision criteria and consultative mechanisms to support declarations of grid security emergencies.

### Threats That Can Trigger Grid Security Emergencies: Implications for Emergency Order Design

A broad array of natural and man-made hazards, including earthquakes and severe weather events such as hurricanes and ice storms, can cause multistate blackouts. However, in amending the FPA, Congress specified that only a limited set of threats can trigger a grid security emergency. They include the “occurrence or imminent danger” of:

(A)

(i) a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure;<sup>56</sup> and

(ii) disruption of the operation of such devices or networks, with significant adverse

<sup>55</sup> 16 U.S.C. § 824o–1, (b)(6).

<sup>56</sup> The second section of this report defines critical electric infrastructure and defense critical electric infrastructure and analyzes their application to the development of grid security emergency thresholds.

effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event;

or

(B)

(i) a direct physical attack on critical electric infrastructure or on defense critical electric infrastructure; and

(ii) significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.<sup>57</sup>

Protecting critical and defense critical electric infrastructure against each of these threats will require different types of emergency orders—though some potential orders may be useful against multiple hazards. The threats will also pose disparate challenges for determining whether a grid security emergency is imminent or under way. Emergency order designs should account for these challenges and provide practical options to protect grid reliability even when the president faces uncertainties about the likelihood and potential consequences of a grid security emergency.

### Geomagnetic Storms as a Possible Initial Focus

Emergency orders for geomagnetic disturbances will entail fewer design challenges than those for cyber attacks and other man-made hazards, and therefore provide opportunities for rapid progress. Geomagnetic disturbance events occur when coronal mass ejections on the sun create geomagnetically induced currents on the earth's surface. These currents can damage unprotected transformers and other grid infrastructure. Compared with the other threats that can trigger grid security emergencies, determining that there is imminent danger of a geomagnetic disturbance event is straightforward. Satellite data on the intensity and direction of energy released in solar storms will help the president decide whether

to declare a grid security emergency and will provide significant warning before geomagnetically induced currents threaten to damage grid infrastructure.

Industry and government partners can develop emergency orders to take advantage of this warning time. For example, the secretary might order BPS entities to take measures to protect grid reliability against the anticipated effects of geomagnetically induced currents by altering power flows to reduce loading on large power transformers or temporarily disconnecting transformers from the grid.<sup>58</sup>

A strong foundation already exists for drafting such orders. Studies of the effects of geomagnetic disturbances on the power grid have contributed to a detailed understanding of vulnerabilities and consequences, as well as the mitigation measures required to avoid the most severe impacts.<sup>59</sup> Executive Order 13744, *Coordinating Efforts to Prepare the Nation for Space Weather Events* (October 2016), directed the federal government to ensure that it has the capability to predict and detect space weather events and the ability to communicate these assessments to public and private sector stakeholders. The order also requires the development of protection and mitigation plans for critical infrastructure and plans for response and recovery if geomagnetic disturbances occur. In addition, the order requires sector-specific agencies to “assess their executive and statutory authority, and limits of that authority, to direct, suspend, or control critical infrastructure operations, functions, and services before, during, and after a space weather event.”<sup>60</sup>

NERC reliability standards provide an additional cornerstone for developing emergency orders for geomagnetic disturbances. TPL-007-1—*Transmission System Planned Performance for Geomagnetic*

<sup>58</sup> Phillips, “Solar Shield.” See also MISO, *Geomagnetic Disturbance Operations Plan*, 5.

<sup>59</sup> See “NOAA Space Weather Scales,” NOAA; and Kappenman, *Geomagnetic Storms*.

<sup>60</sup> Obama, *Executive Order—Coordinating Efforts*.

<sup>57</sup> 16 U.S.C. § 824o–1, (a)(7).

*Disturbance Events* establishes long-lead geomagnetic disturbance planning, including vulnerability assessments, system modeling, performance benchmarks, and a design basis threat for geomagnetic disturbance events.<sup>61</sup> EOP-010-1—*Geomagnetic Disturbance Operations* also requires reliability coordinators to develop geomagnetic disturbance mitigation plans and operating procedures, including specific actions that transmission operators must take based on predetermined geomagnetic disturbance-related conditions.<sup>62</sup>

Moreover, emergency orders for geomagnetic disturbances will not have to tackle the additional challenges posed by cyber attacks and other man-made triggers for grid security emergencies. The sun will not intentionally hide preparations for a geomagnetic disturbance event or “prepare the battlefield” by secreting disruptive, difficult-to-detect malware on utility networks. Nor will solar flares selectively target especially vulnerable nodes in the grid; corrupt the data that utility personnel need to maintain situational awareness over their systems; conduct information warfare to disrupt power restoration and incite public panic; or execute all the other operations that intelligent, sophisticated adversaries will develop to maximize the disruption of critical and defense critical electric infrastructure.

The relative ease of drafting orders for geomagnetic disturbances makes such efforts a prime starting point for industry–government collaboration. The North American Transmission Forum, in coordination with the ESCC, is already examining opportunities to develop template emergency orders for geomagnetic disturbance events. But the greater degree of difficulty associated with protecting the grid from attacks by Russia, China, and other potential adversaries must not become a rationale to defer the development of emergency orders to counter such threats. Instead,

DOE and its industry partners should consider pursuing a multitrack development process: at the same time that they seek rapid progress on emergency orders for geomagnetic disturbances, they should *immediately* accelerate the long-lead work that will be required to counter each of the man-made threats that can trigger grid security emergencies.

### Cyber and Physical Attacks

This report focuses on supporting the development of emergency orders to protect and restore grid reliability against cyber and physical attacks. In doing so, the report follows the lead of the premier electric industry exercise of grid resilience, GridEx. As in previous versions of this exercise series, GridEx IV (conducted in November 2017) employed a scenario based on large-scale, combined cyber and physical attacks against the US electric system by a highly capable adversary.<sup>63</sup> Such combined attacks could pose severe threats to nationwide grid reliability, over and above those created by cyber or physical strikes alone. Grid security emergency orders that can help power companies protect and restore reliability against combined attacks will be especially valuable for national security. Orders and implementation plans that can help counter such severe threats will also be useful in lesser contingencies, including cyber-only strikes.

Current US policy priorities focus on the need to strengthen cyber resilience for the power grid and other critical infrastructure. The US *National Security Strategy* warns that cyber weapons “enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces.”<sup>64</sup> DOE and its partner utilities should prioritize the development of emergency

<sup>61</sup> NERC, *TPL-007-1*.

<sup>62</sup> The standard, however, does not explicitly lay out what those predetermined conditions should be. See NERC, *EOP-010-1*. For an example of geomagnetic disturbance plans, see PJM, *PJM Manual* 13, 69–71.

<sup>63</sup> GridEx includes participation by over one hundred power companies and other components of the electricity subsector. See NERC, *Grid Security Exercise GridEx IV*, vii.

<sup>64</sup> White House, *National Security Strategy*, 12, 27.



orders to counter such attacks, and supplement the mandatory and increasingly stringent cyber critical infrastructure protection standards, as well as voluntary measures that go above and beyond those NERC requirements.<sup>65</sup>

However, orders can also help build resilience against physical attacks on the grid. Since the coordinated attack on the Metcalf substation near San Jose, California, in April 2013, grid owners and operators have taken extensive measures to protect critical electric infrastructure from kinetic attack by high-powered rifles or other weapons. This includes NERC's *CIP-014-2—Physical Security* standard, which outlines the requirements for protecting grid infrastructure from physical attacks.<sup>66</sup> Those measures need to continue. If adversaries can physically destroy large power transformers at critical substations in multiple states, they may be able to create exceptionally wide-area, long-duration outages, given the many weeks that will typically be required to transport and install replacement transformers. Such blackouts could have catastrophic effects on national security and public health and safety.

An adversary would face greater risks when launching physical attacks than cyber attacks. Blowing up transformers and killing workers who are transporting replacement equipment might rapidly escalate conflict with the United States into larger-scale kinetic warfare. In contrast to the typically less visible (and more difficult to detect) malware that cyber adversaries would hide on utility networks, arming and prepositioning covert teams to conduct physical attacks would also increase the risk that the United States would discover the attackers before they struck.

Yet, the potential rewards of physical attacks are immense, especially if the adversary believes that they will create power outages that last far longer than those induced by cyber weapons alone. Emergency orders should be designed to help alter this risk-reward calculus in our favor. If orders can help power companies protect their systems from impending physical attacks, especially in partnership with state and local law enforcement agencies, state National Guard personnel, and other sources of assistance, adversaries may be less willing to accept the risks of preparing and conducting such attacks. And if physical attacks nevertheless occur, the ability to counter them will have major benefits for protecting and restoring grid reliability.

Adversaries may also simultaneously employ both cyber and physical attacks. Such combined attacks can synergistically disrupt the grid in ways that cyber or physical attacks on their own cannot. For example, as in the response to cyber attacks on Ukraine's power grid in 2015, utilities may be able to rapidly restore power by sending personnel to malware-infected substations to manually control grid operations.<sup>67</sup> However, physical attacks that destroy critical substation components or target utility workers will obviate such easy fixes and require much more complicated response plans and capabilities.

The GridEx IV scenario highlighted the unique challenges posed by combined attacks and opportunities to address them. That scenario also assumed that adversaries will wage information warfare campaigns on social media to disrupt restoration operations, inflame public fears, and create challenges for public messaging that are far more difficult to counter than in any past US power outage.

This report adopts a similarly severe threat for analyzing possible emergency orders. In particular, the report examines how orders can protect or restore grid reliability against the combined use of cyber weapons, physical attacks, and information

---

<sup>65</sup> NERC has mandatory standards for critical infrastructure protection against cyber threats. See "United States Mandatory Standards," NERC.

<sup>66</sup> DOE, *Quadrennial Energy Review*, 4–34; and NERC, *CIP-014-2*.

---

<sup>67</sup> E-ISAC and SANS-ICS, *Analysis of Cyber Attack*, v.

warfare against critical and defense critical electric infrastructure. Of course, separate types of emergency orders will be required for physical and cyber threats. Orders to deploy specific countermeasures against unmanned aerial vehicle attacks on substations will be of limited value for ramping up defenses against malware on utility networks. Nevertheless, following GridEx's lead, utilities can also benefit from examining how emergency orders could help them defeat combined attacks, and how they can integrate both cyber and physical defense operations.

The study does not examine options for developing emergency orders against electromagnetic pulse (EMP) attacks. EMP threats pose a significant potential risk to the grid, and a growing (though still relatively small) number of utilities are hardening their critical systems against EMP effects.<sup>68</sup> DOE's EMP strategy provides a valuable framework and approach for managing the risks that EMP threats pose to the grid and other energy systems.<sup>69</sup> DHS's EMP strategy does the same for a broad range of infrastructure sectors.<sup>70</sup> Industry partners such as the Electric Power Research Institute are also making notable contributions to the shared understanding of EMP effects on the grid.<sup>71</sup> However, significant

research is still required to understand the combined effects of EMP wave components on grid hardware and system-wide operations and for cost-effective mitigation options and preparedness planning.<sup>72</sup> As that research progresses, opportunities to develop emergency orders against EMP attacks will grow as well.

## Thresholds for Declaring Grid Security Emergencies<sup>73</sup>

The FPA authorizes the president to declare a grid security emergency when there is "imminent danger" of an attack or when attacks are already occurring. However, the FPA does not further define imminent, nor provide any criteria to help determine whether the anticipated likelihood of an attack is sufficient to warrant an emergency declaration. As will be discussed below, the FPA provides guidance on the potential severity of imminent or ongoing attacks that would constitute a grid security emergency. However, those guidelines are broad and could be subject to starkly different interpretations in future crises.

Some degree of ambiguity is useful. Preserving wide presidential latitude for declaring grid security emergencies will be essential to deal with unforeseen challenges and to avoid locking US crisis managers into rigid positions that adversaries might exploit. In particular, it would be risky to publicize explicit red lines that would trigger a declaration. Adversaries might be tempted to conduct operations just below those levels if they believed doing so would delay US defensive measures, including the issuance of emergency orders to safeguard the grid. Adversaries might even seek to spoof the president into declaring a grid security emergency when they had no intention of launching an attack—especially if adversaries believed doing so might prompt the issuance of disruptive emergency orders, crash utility stock

---

<sup>68</sup> In high-altitude EMP attacks that threaten the grid, adversaries would detonate nuclear weapons in the atmosphere above the United States to create waves of electromagnetic energy. This blast includes multiple disruptive components, one of which creates effects (and has protection requirements) similar to geomagnetic disturbances. The early-time component threatens grid infrastructure in a way that is unique to EMP attacks and requires special protection measures. See EPRI, *Electromagnetic Pulse and Intentional EMI Threats*, 3-3–3-4.

<sup>69</sup> DOE set strategic goals for addressing EMP threats and created an action plan to meet those goals. DOE, *Electromagnetic Pulse Resilience Action Plan*. The fiscal year 2017 National Defense Authorization Act directed DHS to create a similar strategy, which is currently in draft form. See National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328. The EPRI continues to lead electric industry research on EMP threats to the grid and potential mitigations. EPRI, *High-Altitude Electromagnetic Pulse*.

<sup>70</sup> DHS, *Strategy for Protecting and Preparing*.

<sup>71</sup> EPRI, *Electromagnetic Pulse and Intentional EMI Threats*.

<sup>72</sup> INL, *Strategies, Protections, and Mitigations*.

<sup>73</sup> The analysis in this section builds on the findings of Stockton, "Thresholds."

prices, or incite public panic in ways that they would find politically useful.

Nevertheless, power companies and other grid resilience stakeholders have argued that more clarity in triggers and thresholds would be helpful, especially in terms of understanding the scale and severity of the events that emergency orders should be designed to help counter.<sup>74</sup> Federal officials could also find it useful to have decision criteria to help frame their own internal deliberations and recommendations to the president. In an intense crisis, ambiguities in the FPA could fuel disagreements among the president's advisors as to whether the threat of attack was sufficiently severe to declare a grid security emergency. Developing a decision framework to support the declaration process could facilitate consensus-building and provide a structured way to integrate data on attack indicators. However, in adopting such a framework, it would also be prudent to avoid revealing any specific declaration triggers or thresholds for adversaries to exploit in their attack planning.

The section that follows examines two factors that a decision framework might encompass: the likelihood of an attack occurring and its potential consequences. This section also examines how improved information sharing between government agencies and power companies can support these assessments and recommends industry–government consultations in the declaration process that go beyond the existing provisions of the FPA.

### **Determining When Attacks Are Imminent: Criteria for Declaring Grid Security Emergencies**

In key respects, the BPS is under cyber attack today. Russia and other nations are conducting sustained, increasingly sophisticated campaigns to implant advanced persistent threats on utility systems. These campaigns can enable adversaries to maintain a covert presence on BPS networks, secrete malware

designed to disrupt grid operations, and conduct other malicious activities to prepare for possible attacks on critical system components.<sup>75</sup> PJM Interconnection's former CEO Terry Boston recently stated that the company experiences three thousand to four thousand hacking attempts *every month*.<sup>76</sup> Penetration efforts on a similarly massive scale are likely occurring against BPS entities across the United States. While many of these efforts target information technology systems not directly involved in operating the grid, malware implants on operational technology systems are increasingly frequent and sophisticated.<sup>77</sup> And, as in the case of BlackEnergy and other campaigns against utility networks, many of these efforts have successfully embedded malware that adversaries could use to strike the grid at any moment.<sup>78</sup> The net result, according to US director of national intelligence Dan Coats: "Today, the digital infrastructure that serves this country is literally under attack."<sup>79</sup>

Of course, there is a huge gulf between implanting destructive malware on the grid and using that malware to create blackouts. The Trump administration has promised to impose "swift and costly consequences" on foreign governments and other actors who undertake "significant malicious cyber activities" against US critical infrastructure.<sup>80</sup> Attacks that create massive power outages and jeopardize US national security would be especially likely to provoke such a response. However, the president does not need to wait for blackouts to occur before declaring

<sup>75</sup> "Alert (TA18-074A)"; "Alert (TA17-293A)"; Defense Science Board, *Task Force on Cyber Deterrence*, 4; and ICF International, *Electric Grid Security and Resilience*, 19.

<sup>76</sup> Dougherty, "Biggest U.S. Power Grid Operator Suffers Attacks."

<sup>77</sup> "Alert (TA17-293A)"; and "Alert (TA18-074A)."

<sup>78</sup> BlackEnergy persisted on utility industrial control systems for at least three years before being detected in 2014. A more virulent form of BlackEnergy inflicted the 2016 blackout on Ukraine. "Alert (ICS-ALERT-14-281-01E)."

<sup>79</sup> Barnes, "Warning Lights."

<sup>80</sup> White House, *National Security Strategy*, 13.

<sup>74</sup> Paradise et al., "ISO-RTO Council Comments," 2.

a grid security emergency. The “imminent danger” of attack is sufficient to declare an emergency and for the secretary to issue orders to help utilities ramp up their defenses.

Implants of new, potentially devastating malware across the electric grid could help the president make such a determination, particularly if other warning indicators suggest that cyber attacks are becoming increasingly likely. The geopolitical context in which cyber attacks might occur provides one such indicator. It is (barely) conceivable that adversaries will launch a “bolt from the blue” attack on the grid without any preceding rise in tensions with the United States. However, it is far more likely that adversaries will strike in the context of an escalating crisis in Northeast Asia, the Baltics, or some other region and attack the grid to disrupt the deployment of US forces to the region or to achieve other military and political goals.<sup>81</sup> Evidence that adversaries are ramping up their efforts to embed sophisticated malware across BPS networks, and are taking other measures that position them to cause multistate blackouts, should carry greater weight in a crisis environment.

Policy makers should consider developing a framework to assess whether these cyber preparations help justify the declaration of a grid security emergency. The US Office of the Director of National Intelligence (ODNI) has issued a cyber threat framework that could support such development efforts. The ODNI notes that government agencies, academia, and the private sector are using over a dozen analytic models to categorize cyber threats and identify changes in the activities of cyber adversaries. ODNI’s framework is intended to provide a common basis for characterizing threat activity to support analysis and senior-level decision-making.<sup>82</sup> Figure 2 illustrates the cyber threat framework.

<sup>81</sup> The section on preattack grid security emergency declarations examines these national security-related issues and their implications for designing emergency orders.

<sup>82</sup> “Cyber Threat Framework,” ODNI; and ODNI, *Common Threat Framework*, 5.

The initial stage of adversary activity is to prepare for conducting malicious activity. Adversaries then engage and establish presence on targeted systems, allowing them to “operate at will.” In the final stages, attackers seek to destroy grid hardware, software, and/or data, and prepare to conduct follow-on operations as needed to magnify the extent and duration of their disruptive effects.<sup>83</sup>

If adversaries were to suddenly make new moves into the penultimate phase (operate at will) during an intense political crisis or regional confrontation, evidence that they had done so could help the president determine whether attacks were imminent. Other independent sources of data could provide additional context for assessing adversary moves toward more threatening preattack stages. James Miller, former undersecretary of defense for policy, notes that “the United States devotes massive resources to human and technical intelligence collection of our potential adversaries.”<sup>84</sup> Such indicators could contribute to overall assessments of attack imminence.

Policy makers might also supplement the cyber threat framework with specialized attack models for the industrial control systems and other grid components that are crucial for electric system operations. The Industrial Control System Cyber Kill Chain provides an especially promising opportunity to do so. The kill chain identifies the specific sequenced phases that adversaries execute to conduct attacks that inflict predictable physical effects on grid equipment and operations.<sup>85</sup> Stage 1 begins with planning and reconnaissance against

<sup>83</sup> ODNI, *Common Threat Framework*, 13, 16.

<sup>84</sup> Miller, “Cyber Deterrence.”

<sup>85</sup> The Industrial Control System Cyber Kill Chain is adapted from the Cyber Kill Chain™ model developed by Lockheed Martin analysts Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin in 2011 to “help the decision-making process for better detecting and responding to adversary intrusions.” The Industrial Control System Cyber Kill Chain tailors that decision-making tool for industrial control system-specific cyber threats and consequences. See Assante and Lee, *Industrial Control System Cyber Kill Chain*.



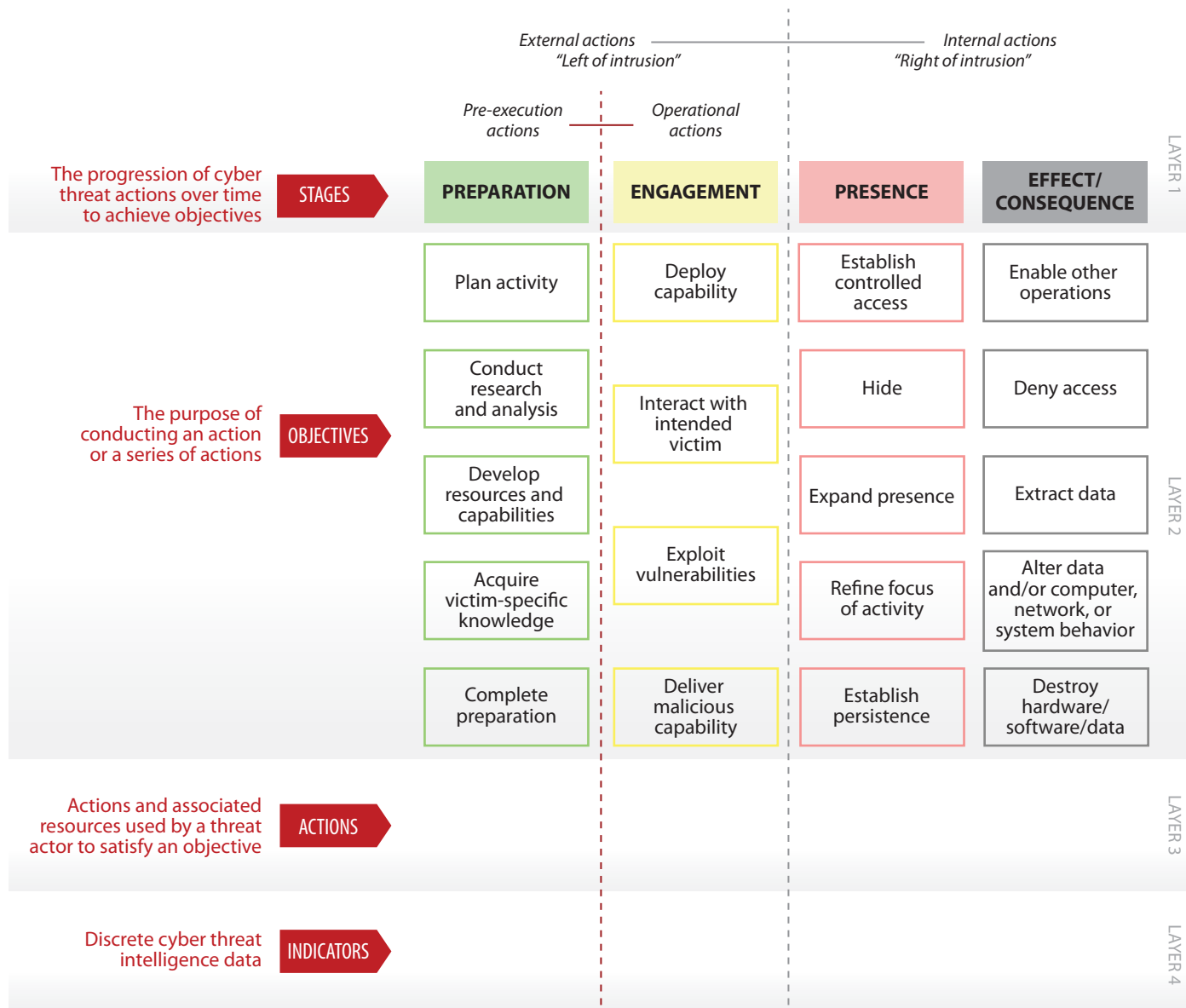


Figure 2. ODNI Cyber Threat Framework

industrial control system networks and includes intrusion and enablement phases. In stage 2, the attacker uses the knowledge gained in stage 1, developing and testing attack capabilities, and—ultimately—executing the attack. Evidence of an adversary's position along this kill chain could help support decision-making on the imminence of potential attacks, with the final phases posing the most proximate indications that an adversary is poised to strike the grid.

### Potential Attack Consequences

The imminence of an attack provides only one possible criterion for declaring a grid security emergency. A second would be the potential consequences of the attack. Indeed, when Congress defined grid security emergencies in the FPA, legislators established at least implicit, consequence-based thresholds for declaring an emergency. The FPA defines grid security emergencies as occurring when attacks that are imminent or under way "could disrupt the

General Definition		Observed Action	Intended Consequence
Level 5: Emergency (Black)	<i>Poses on imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons</i>	Effect	Cause physical consequence
Level 4: Severe (Red)	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties</i>		Damage computer and networking hardware
Level 3: High (Orange)	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>	Presence	Corrupt or destroy data  Deny availability to a key system or service
Level 2: Medium (Yellow)	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>	Engagement	Steal sensitive information
Level 1: Low (Green)	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence</i>		Commit a financial crime
Level 0: Baseline (White)	Unsubstantiated or inconsequential event	Preparation	Nuisance denial of service or defacement

Figure 3. Elements of the Cyber Incident Severity Schema

operation” of devices or networks that are “essential to the reliability of critical electric infrastructure or defense critical electric infrastructure.”<sup>86</sup>

However, the FPA does not clarify the extent of disruption that should trigger the declaration of an emergency. Some grid resilience stakeholders have expressed concern that policy makers might set the threshold too low, and declare grid security emergencies for minor incidents. For example, the ISO/RTO Council proposes that the use of emergency orders in such an emergency “should be reserved for true widespread emergencies.”<sup>87</sup> But

neither Congress nor DOE have yet specified what higher-level thresholds might be appropriate.

One approach to account for the potential consequences of an attack would be to leverage existing federal criteria for categorizing cyber events by the severity of their effects. The definition of “significant cyber incidents” in Presidential Policy Directive 41, *United States Cyber Incident Coordination*, provides a starting point to do so. Under the directive, significant cyber incidents are those that are “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or

<sup>86</sup> 16 U.S.C. § 824o-1, (a)(7).

<sup>87</sup> Paradise et al., “ISO-RTO Council Comments,” 2.



public health and safety of the American people.”<sup>88</sup> Policy makers could apply this demonstrable-harm standard to support decisions on whether to declare a grid security emergency. If officials determine that a cyber attack is likely to inflict such harm, their finding would provide a compelling justification for making an emergency declaration.

The December 2016 *National Cyber Incident Response Plan*’s cyber incident severity schema offers a still more detailed basis to assess attack consequences. The schema (Figure 3) serves as “a common framework and shared understanding to evaluate and assess cyber incidents at all federal departments” and agencies.<sup>89</sup> Policy makers could use the schema to help develop consequence-based criteria for declaring grid security emergencies. For example, if assessments suggest that an attack is likely to create a “level 5 emergency,” which poses “an imminent threat to the provision of wide-scale critical infrastructure services, national [government] stability, or to the lives of U.S. persons,” the declaration of a grid security emergency should be near-automatic. Level 4 events would also be very strong candidates for justifying such declarations. However, as with all such criteria, the president should also retain the latitude to make declarations for less severe incidents (for example, the disruption of a cluster of major defense installations).

One advantage of leveraging these government-wide standards is that doing so can help integrate decisions on grid security emergencies into the broader US system for incident response. As officials update the *National Cyber Incident Response Plan* and its supporting severity schema, valuable opportunities will emerge to ensure that grid security emergency declarations and operations are part of a broader, multisector approach to strengthening infrastructure preparedness.

### **Grid-Specific Criteria for Assessing Attack Consequences: Building on Standards for Adequate Levels of Reliability**

If policy makers rely only on general, government-wide decision criteria, they will miss opportunities to take advantage of the electric industry’s standards for assessing the severity of threats to grid reliability. NERC has carefully defined what constitutes adequate reliability for the power grid, as well as the types of large-scale reliability failures that owners and operators need to prevent. If utilities and government agencies have the data and analytic tools necessary to determine whether adversaries’ attacks will create such failures, their assessments could provide valuable input into decisions on declaring grid security emergencies.

The 2003 Northeast blackout spurred NERC’s efforts to define adequate levels of grid reliability and specify the types of system failures that BPS entities need to prevent. In response to that outage, which created cascading power failures over wide areas of the United States and Canada, Congress enacted comprehensive amendments to the FPA to help prevent equivalent grid failures in the future. The 2005 amendments required FERC to certify an electric reliability organization, which will have “the ability to develop and enforce . . . reliability standards that provide for an adequate level of reliability of the bulk-power system.”<sup>90</sup> However, the FPA never defined *adequate level of reliability*; that task was left to the electric reliability organization.

When NERC became the electric reliability organization in 2006, defining the adequate level of reliability was one of its first initiatives. NERC’s board of trustees approved an initial definition for the “characteristics of a system with an adequate level of reliability” in 2008, which was updated in 2013.<sup>91</sup> Three components of NERC’s definition—cascading failures, uncontrolled separation, and instability—are

<sup>88</sup> Obama, *United States Cyber Incident Coordination*.

<sup>89</sup> DHS, *National Cyber Incident Response Plan*, 29–30.

<sup>90</sup> 16 U.S.C. § 824o, (c)(1).

<sup>91</sup> NERC, *Technical Report*, 17.

especially useful to help assess the potential severity of imminent or ongoing attacks against the BPS.<sup>92</sup>

The sections that follow examine these three components, the reliability failures they can entail, and implications for declaring grid security emergencies. Subsequent portions of the report analyze options to develop emergency orders tailored to prevent such failures. However, in grid security emergencies, risks of all three types of failures might emerge in rapid succession and would be inextricably linked.

**Cascading failures.** NERC defines cascading as “the uncontrolled successive loss of system elements triggered by an incident at any location.” Such cascading “results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.”<sup>93</sup> NERC’s definition states that a system is adequately reliable if the system will not experience cascading failures when struck by lightning or affected by other frequent, predictable incidents (i.e., “predefined Disturbances”). But more severe events have caused instabilities that led to cascading in the past and may do so again—especially if adversaries design coordinated cyber and physical attacks to spread blackouts across multiple utilities.

The 2003 blackout illustrates the speed with which failures can cascade. That blackout, which affected approximately fifty million people across the United States and Canada, started with a relatively minor incident. On a hot day in August, multiple 345-kilovolt transmission lines tripped after sagging into overgrown trees. With proper situational awareness, operators might have been able to take actions to handle such a contingency, but failures in

the utility’s control room alarm processor resulted in operators being entirely unaware of the problem. In an unfortunate coincidence, the utility’s reliability coordinator also had computer problems and lacked the visual tools necessary to support grid operators.<sup>94</sup> These failures shifted power flows to a system of 138-kilovolt lines, which were unable to handle the added current flows, and overloaded the last remaining 345-kilovolt path into the area, beginning the major, uncontrollable cascading sequence.<sup>95</sup> This sequence tripped over five hundred generating units and four hundred transmission lines in only eight minutes—with most of these failures occurring *in the last twelve seconds* of the cascade.<sup>96</sup>

As in the case of the 2003 blackout, cascading failures can be initiated by natural hazards, operator errors, and other factors unrelated to adversarial attacks. But cyber and physical attacks could also be tailored to spark and rapidly spread cascading blackouts by destroying critical generation and transmission nodes; alter protective relay settings so that grid components trip offline (or fail to do so) in ways that intensify the outages; deny grid operators the data and situational awareness needed to operate their own systems and cope with contingencies in surrounding systems; and take other measures designed to produce cascading failures.<sup>97</sup> Indeed, adversaries may seek to replicate some of the factors that made the 2003 blackout so severe—particularly by denying or corrupting situational awareness data.

The imminent danger or occurrence of adversary-induced cascading outages could be a criterion for declaring a grid security emergency. Cascading blackouts that spread across multiple regions of the United States (as in 2003) would be certain to disrupt

<sup>92</sup> See section 215 of the FPA, which defines *reliable operation* as “operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.” 16 U.S.C. § 824o, (a)(4).

<sup>93</sup> NERC, “Informational Filing,” 1, 7.

<sup>94</sup> NERC Steering Group, *Technical Analysis of Blackout*, 27–28.

<sup>95</sup> NERC Steering Group, *Technical Analysis of Blackout*, 27–28.

<sup>96</sup> NERC Steering Group, *Technical Analysis of Blackout*, 109.

<sup>97</sup> Cherepanov and Lipovsky, “Industroyer”; Sistrunk, “ICS Cross-Industry Learning”; “Alert (TA17-163A)”; and Dragos, *CRASHOVERRIDE*, 24.

the operation of grid devices and networks essential to critical and defense critical electric infrastructure—on a massive scale. Those disruptive effects will be still greater if attackers destroy transformers and other grid infrastructure to extend the duration of the blackout.

**Uncontrolled separation.** NERC defines uncontrolled separation as “the unplanned loss of BES elements resulting in islanding and possible unplanned BES load loss.”<sup>98</sup> Severe events “resulting in the removal of two or more BES elements with high potential to cascade” can produce uncontrolled separation.<sup>99</sup>

Uncontrolled separation almost always occurs in conjunction with cascading failures. In the 2003 blackout, uncontrolled separation led to the creation of large electrical islands that “quickly became unstable after the massive transient swings and system separation” because there was insufficient generation within the islands to meet electricity demand.<sup>100</sup> Similar sequences occurred in previous major blackouts. In the July 1977 New York City blackout, for example, a string of trips and failures caused the Consolidated Edison system to separate from surrounding systems and collapse.<sup>101</sup> In the 1982 West Coast blackout, loss of 500-kilovolt lines activated a scheme to achieve controlled separation, but failure of that system as well as the backup scheme caused uncontrolled separations, dividing the system into four unplanned islands.<sup>102</sup> A similar blackout in the same region in 1996, triggered by multiple major transmission line outages, again separated the Western Interconnection into four electrical islands

“with significant loss of load and generation.”<sup>103</sup> The onset of adversary-induced uncontrolled separation would provide a clear-cut basis for declaring the existence of a grid security emergency, if cascading failures had not already prompted the president to make such a determination.

**Instability.** NERC defines system instability as “the inability of the Transmission system to remain in synchronism . . . characterized by the inability to maintain a balance of mechanical input power and electrical output power following a Disturbance on the BES.”<sup>104</sup> The BES can experience frequency, voltage, or angular instability—though none should occur during normal operating conditions.<sup>105</sup>

Severe natural hazards and other disturbances can create temporary instabilities. Grid protection systems and operational protocols typically mitigate their disruptive effects. However, more severe instabilities can result in cascading failures and uncontrolled separation. Specifically, the transmission system may experience large power swings if BPS generators accelerate or decelerate too much during a disturbance, causing transmission lines to trip and generators to go out of step and trip offline, and resulting in further acceleration and deceleration—or both.<sup>106</sup> Once a portion of the grid experiences such instability, it is extremely hard to manually contain.

Adversaries could design attacks to exacerbate grid instabilities and disrupt synchronization as part of a broader strategy to create widespread cascading failures. For example, adversaries may seek to compromise the protection systems necessary to automatically correct instabilities when they occur. Corrupting or disabling protection systems could also make critical grid components vulnerable to physical damage from enemy-induced power surges.

<sup>98</sup> NERC, “Informational Filing,” 6.

<sup>99</sup> NERC, “Informational Filing,” 13.

<sup>100</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 75.

<sup>101</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 104.

<sup>102</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 105.

<sup>103</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 106.

<sup>104</sup> NERC, “Informational Filing,” 6.

<sup>105</sup> NERC, “Informational Filing,” 1–2.

<sup>106</sup> NERC, “Informational Filing,” 6.

Evidence that adversaries were taking preparatory measures to create widespread instabilities could help the president determine that a grid security emergency exists.

However, it may be difficult to predict whether an impending attack will create such failures. The first requirement to do so will be to determine the extent to which adversaries have embedded advanced persistent threats or established other means of attack across the grid—a task that adversaries will complicate by attempting to hide their malware from detection. The next step will be to rapidly characterize these threats, assess the vulnerability of utility systems to them, and predict the consequences for grid reliability if the enemy strikes. Such assessments will also need to account for system-wide effects involving the interaction of multiple adversary-induced disruptions, which may compound and reinforce instabilities in ways that are difficult to predict. PJM Interconnection, LLC, the regional transmission operator for much of the Mid-Atlantic and some neighboring states, recently noted that “additional study is needed to better understand the expected impacts of a large-scale cyber-attack.”<sup>107</sup> Given these challenges, it may be difficult to fully predict the potential impact of cyber attacks on grid reliability until attacks are well under way.

But it could also be risky to wait until attacks are occurring to declare a grid security emergency. In the 2003 Northeast event, for example, cascading blackouts spread across vast areas in seconds. If the president delays declaring a grid security emergency until cascades are under way, emergency orders designed to help prevent their spread may come too late. A better option might be to make an early decision based on imperfect assessments, especially if (as this report recommends) DOE can issue preattack emergency orders that will bolster grid defenses without disrupting normal electric service.

In particular, the president could consider declaring a grid security emergency if (1) an attack appears to be increasingly likely, and (2) assessments indicate that the impending attack may create cascading blackouts or other widespread instabilities. Figure 4 illustrates one option for developing a decision support framework that accounts for the likelihood and potential consequences of an attack. The vertical axis depicts the ODNI cyber threat framework’s four stages of adversary actions, from potential attack preparations to actual strikes against the grid. An adversary’s sudden, large-scale moves up this axis—especially in the context of a severe international crisis—could help the president determine that an attack is impending. The horizontal axis represents the risk that if an attack occurs, the grid will experience cascading failures and other widespread instabilities that would inflict demonstrable harm to national security, the economy, or public health and safety. Attacks that pose little or no risk of cascading blackouts might not warrant the declaration of a grid security emergency.

However, systemic threats to grid reliability are far from the only consequence-based criteria that the president might want to consider. More narrowly targeted attacks to disrupt the flow of power to an area vital to the economy or to national security, such as the National Capital Region, might be sufficient to declare a grid security emergency. Policy makers could develop more refined decision frameworks to account for a broad array of consequence thresholds, as well as further criteria for assessing attack imminence.

## Data Sharing and Consultations with Industry

The electric industry can provide data and analytic support to help the president and other officials decide whether to declare a grid security emergency. Power companies will have direct access to the malware that adversaries implant on their networks, and will be well positioned to assess the potential

<sup>107</sup> PJM, “Comments and Responses,” 35.



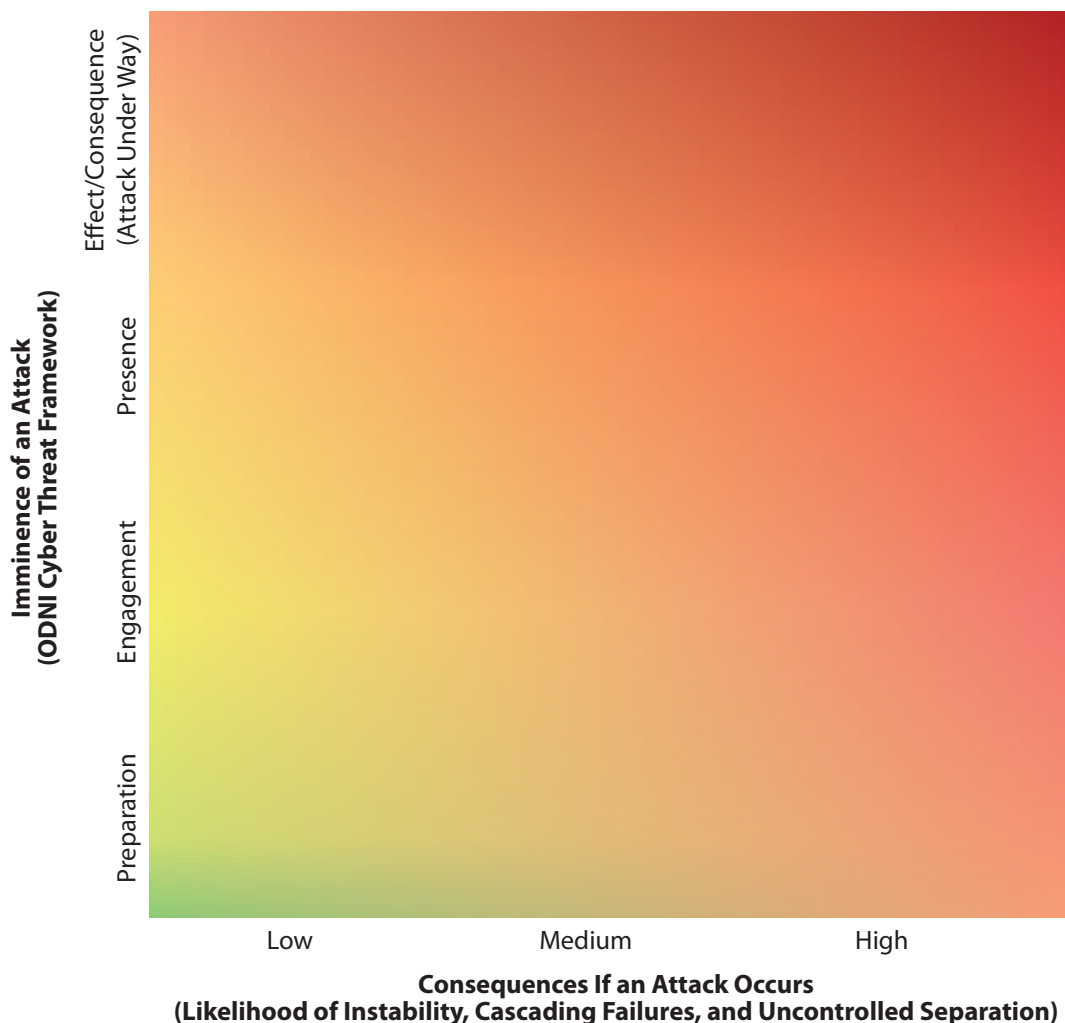


Figure 4. Notional Decision Framework for Declaring Grid Security Emergencies

impact of various attack vectors on their systems and on the grid as a whole.

Government agencies and cyber contractors can help utilities target searches for this malware and provide additional value for the declaration process. If a regional crisis or other geopolitical factors increase the risk of cyber attacks on the grid, agencies should be prepared to ramp up information sharing with BPS entities, especially in terms of specific signatures or other threat indicators to search for in utility networks, logs, and critical equipment.

Industry and government should also explore how ongoing threat detection and analysis initiatives could directly help assess the imminence and

potential consequences of attacks. For example, DOE has projects under way to bolster situational awareness for operational technology networks that could be applied to support such assessments. The department is developing capabilities to monitor traffic on operational technology networks via the Cybersecurity for the Operational Technology Environment project.<sup>108</sup> Other department-funded projects could prove useful for the emergency declaration process as well.<sup>109</sup>

<sup>108</sup> DOE, *Multiyear Plan*, 23.

<sup>109</sup> See, for example, the Containerized Application Security for Industrial Control Systems, Survivable Industrial Control Systems, and Research Exploring Malware in Energy Delivery Systems projects. “Sandia’s Grid Modernization Program

Utilities and DOE might also refine ongoing information sharing initiatives to directly support the emergency declaration process. For example, DOE's Cybersecurity Risk Information Sharing Program is a public-private partnership to build bidirectional situational awareness and facilitate classified and unclassified information sharing.<sup>110</sup> DOE's 2018 cybersecurity plan launched additional activities to advance industry participation in the program, as well as its analytic tools and capabilities.<sup>111</sup> The program is managed by NERC and the E-ISAC, which play an integral role in sharing information and establishing situational awareness within the electricity subsector.<sup>112</sup> In addition, FERC recently issued a proposed directive for NERC to expand reporting requirements for cyber incidents, including for those that "might facilitate subsequent efforts to harm the reliable operation of the bulk electric system."<sup>113</sup> All of these efforts could be integrated to support assessments of the likelihood and potential consequences of attacks.

DHS's May 2018 cybersecurity strategy provides a broader approach to expand information sharing. Most important, the strategy could enable data from other infrastructure sectors to support the declaration process, especially from communications systems and other sectors that support power restoration operations. The strategy also calls for the expansion of automated mechanisms to receive, analyze, and share cyber threat indicators, defensive measures, and other cybersecurity information with critical infrastructure and other key stakeholders.<sup>114</sup>

Such automated sharing mechanisms will be vital to accelerate the identification and assessment of malware that could pose imminent threats to grid reliability. DHS's Automated Indicator Sharing capability "enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed."<sup>115</sup> This bidirectional information sharing will limit an adversary's ability to compromise multiple systems with the same malicious code. The Defense Advanced Research Projects Agency is also working on new technologies to protect the grid. In particular, the agency's Rapid Attack Detection, Isolation and Characterization Systems (RADICS) program is working with companies to develop prototype capabilities for improving attack detection, response, and forensics support.<sup>116</sup> Moreover, as automated malware detection and analytic techniques improve, utilities may be able to speed their evaluation of potential intrusions and slash the number of false positives that current detection systems generate.<sup>117</sup> All of these initiatives should be leveraged to help the president determine whether to declare a grid security emergency.

Policy makers should also consider preplanning to consult with grid owners and operators in the declaration process. The FPA leaves the president with sole authority to declare a grid security emergency. If a potential emergency surfaced, the president would almost certainly draw on the expertise and recommendations of the secretary of energy, as well as other members of the National Security Council and supporting agencies. But power companies and their industry organizations will also have perspectives on operational and technical issues that could prove valuable for assessing potential attacks.

---

Newsletter," Sandia National Laboratories; and "REMEDIYS," Cyber Resilient Energy Delivery Consortium.

<sup>110</sup> "Energy Sector Cybersecurity Preparedness," DOE.

<sup>111</sup> DOE, *Multiyear Plan*, 23.

<sup>112</sup> "Electricity Information Sharing and Analysis Center," NERC.

<sup>113</sup> FERC, *Cyber Security Incident Reporting Reliability Standards* (161 FERC ¶ 61,291), 2.

<sup>114</sup> DHS, *Cybersecurity Strategy*, 13.

---

<sup>115</sup> "Automated Indicator Sharing (AIS)," US-CERT.

<sup>116</sup> Douris, "DARPA Research."

<sup>117</sup> Ucci, Aniello, and Baldoni, "Survey on Machine Learning," 1:5; McElwee et al., "Deep Learning"; and McElwee, "Probabilistic Cluster."



Neither the FPA nor the grid security emergency rule explicitly provide for consultations with industry on whether to declare a grid security emergency. The FPA calls for consultations “to the extent practicable” before the secretary issues emergency orders.<sup>118</sup> But there are no equivalent provisions to include industry input in the emergency declaration process.

Industry and government partners should explore options to provide for such consultations, preferably by leveraging existing mechanisms under the ESCC and E-ISAC. As with consultations on issuing orders, urgent circumstances could shorten or preclude opportunities for government dialogue with industry on declaring grid security emergencies. Consultations will be especially problematic in the face of “bolt from the blue” attacks. Nevertheless, when a regional confrontation or other crisis creates an increased risk of attacks on the grid, government discussions with industry could be invaluable for determining whether (and when) to declare a grid security emergency.

## Grid Security Emergency Phases and Order Design Options

DOE and its industry partners should consider designing emergency orders for three potential phases of grid security emergencies. First, if the president determines that there is an imminent danger of an attack, the secretary should be ready to issue preattack orders that help utilities protect grid reliability. Second, once attacks are under way, the secretary could issue orders to reduce the risk of cascading failures or other widespread disruptions of electric service. Third, as utilities begin to restore grid reliability, orders could help utilities replace damaged equipment and counter adversary efforts to disrupt restoration operations.

Orders for each phase of a grid security emergency will differ not only in terms of when the secretary would issue them but also in the degree to which they

will disrupt normal electric service. Some orders, such as staffing up emergency operations centers before an attack occurs, would leave customers unaffected. In contrast, orders for prioritized load shedding could temporarily halt service to many customers—but could also greatly reduce the risk that instabilities will lead to cascading blackouts.

Figure 5 provides examples of orders that vary in the degree of disruption they would inflict on normal service, and also in the way they would meet the phase-specific challenges of grid security emergencies. The analysis that follows examines each of them (and other possible orders) in greater detail.

Some emergency orders will be useful in more than one phase of grid security emergencies. For example, emergency orders for maximum generation to increase power reserves and address potential shortfalls in the supply of electricity could be useful both when attacks are imminent and when they are under way. The second and third phases of grid security emergencies are likely to overlap. As soon as power companies “stop the bleeding” from initial attacks and prevent disruptions from spreading across their infrastructure and to neighboring utilities, they will begin operations to restore normal service as quickly as possible. But if adversaries damage or destroy sufficient numbers of large power transformers or other critical equipment, utilities might need to sustain prioritized load shedding and other extraordinary measures long after power restoration operations are under way.<sup>119</sup> Adversaries may also launch follow-on attacks once utilities begin focusing on restoration. Emergency orders to help utilities repel such attacks could become essential components of the restoration process.

<sup>118</sup> 16 U.S.C. § 824o–1, (b)(3).

<sup>119</sup> In examining unprecedentedly severe grid disruptions, NERC identifies the period after the initial event (but before the grid is fully restored to pre-event conditions) as the “new normal”—characterized by “degraded planning and operating conditions unlike anything the industry has ever experienced in North America that could exist for months.” See Severe Impact Resilience Task Force, *Severe Impact Resilience*, 14, 16.

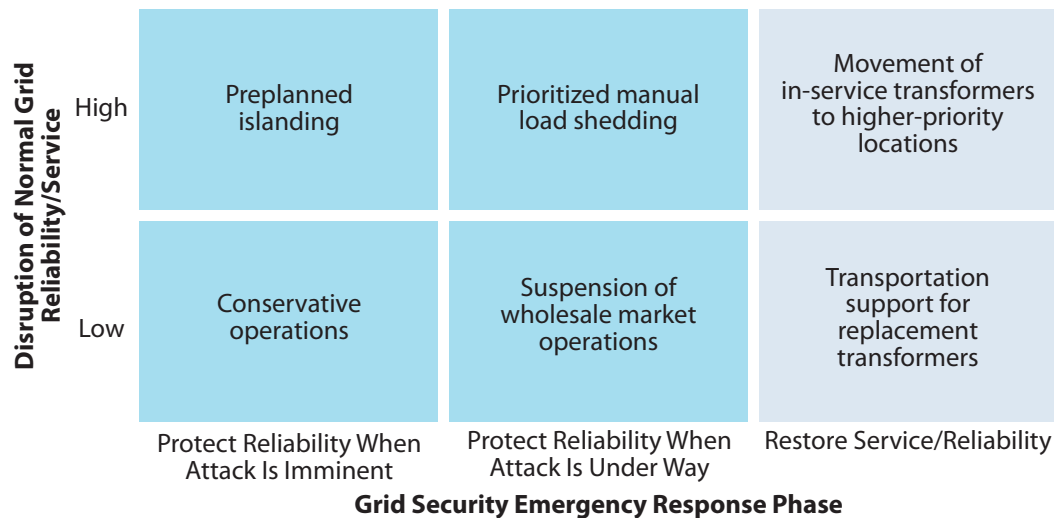


Figure 5. Emergency Order Matrix: Examples of Order Designs

DOE and its partners will need flexibility to deal with the overlapping phases of grid security emergencies. Nevertheless, being able to categorize potential orders in terms of when they would likely be issued and which phases of emergency operations they could support can help establish a systematic process for developing orders.

Creating emergency orders for all three phases can also help utilities and DOE integrate the orders into seamless, multiphase operational plans for grid security emergencies. As intense regional crises or other events elevate the risk of attacks on the grid, it will be prudent to preplan for the issuance of emergency orders for multiple grid security emergency phases. Orders for preattack measures such as conservative operations would be issued first if attacks are deemed imminent. At the same time, however, DOE and the utilities subject to emergency orders should be using any available warning time to prepare for the issuance and implementation of orders for the midattack and restoration phases.

## Preattack Options

Even with industry-provided data and expertise, uncertainties are likely to persist as to whether an attack is genuinely imminent. The *wrong* way to deal

with these ambiguities is to delay the declaration of a grid security emergency until blackouts begin; doing so would forego the benefits of issuing preattack emergency orders. It may be possible to develop orders that will offer significant benefits if adversaries strike yet also have little or no impact on normal service—thereby offering “no-regrets” options to employ when the likelihood of an attack remains uncertain. Industry and government partners should also explore options for the preattack phase that would be more disruptive but also offer potentially far-reaching benefits. These two options occupy the left-hand column in Figure 5.

Conservative operations that utilities employ against natural hazards provide a model for protecting the grid in ambiguous preattack situations. When weather forecasters predict that hurricanes or other severe storms may hit the United States, BPS entities in the potential storm track can adopt conservative operations to help protect the reliability of electric service against high winds and other storm effects and prepare for possible response and restoration operations if grid infrastructure is damaged.<sup>120</sup> For

<sup>120</sup> Conservative operations are not defined in the NERC glossary of terms. However, many reliability coordinators and other BPS entities offer similar definitions of the term. For PJM, conservative operations constitute actions that can be taken to “implement

example, reliability coordinators may direct that additional generation reserves be made available from generation plant owners, increasing the resources available to respond to any unexpected events.<sup>121</sup> Power companies may also cancel noncritical generation and transmission maintenance activities; reduce transfer limits to give the transmission system extra “slack”; and staff their backup control centers, critical BPS substations, and other vital facilities to set the stage for emergency operations as hurricanes approach.<sup>122</sup>

A defining feature of these frequently used conservative operations is that they do not disrupt normal service to customers. Their negligible service impact makes them more viable to implement when the storm’s path remains uncertain. Forecasters cannot predict precisely where a hurricane will make landfall when the storm is days away from the US coast. Instead, they provide a wide “cone of uncertainty” that becomes increasingly narrow as the hurricane approaches. Utilities cannot wait until the hurricane strikes to mobilize backup workers and carry out other conservative operations. To be effective, many such measures must be taken before it is clear that they will actually be needed to protect or restore grid reliability. The fact that these operations do not affect normal service to customers enhances the willingness of utility leaders to order their implementation while the storm track remains uncertain.

---

additional actions to ensure the BES remains reliable in the face of the additional threats” when “events, conditions, or circumstances may put the Bulk Electric System (BES) at an increased level of risk, compared to normal operating conditions.” See PJM, “Conservative Operations,” 3. Similarly, the Western Electricity Coordinating Council, defines conservative systems operations as the operating state where control centers, generation plants, and other infrastructure and personnel assets “are restricted and managed in order to maintain or restore reliability of the power system from the negative influence of a triggering event or condition.” See Western Electricity Coordinating Council, “Conservative System Operations,” 4.

<sup>121</sup> PJM, “Conservative Operations,” 3.

<sup>122</sup> PJM, “Conservative Operations,” 9.

Industry and government partners should borrow from this model to develop orders for preattack conservative operations against cyber and/or physical attacks. Some have already begun to do so. While all major utilities are prepared to implement conservative operations against natural hazards, a handful have gone especially far in adapting conservative operations to meet the specialized challenges posed by cyber and physical threats.<sup>123</sup> This preparation will be extremely helpful as potential attacks loom. As a regional confrontation or other precipitating crisis intensifies, it is conceivable that the US intelligence community will acquire timely and absolutely certain knowledge that adversaries are about to strike the grid. However, it is much more likely that ambiguities will persist about whether the adversary will actually attack and risk a devastating US response. To ensure that sufficient time is available to implement conservative operations, the secretary may need to order the initiation of such measures when enemy intentions remain uncertain—and when warning indicators may turn out to be false.

Many of the conservative operations that will bolster resilience against adversary attacks would be similar to those developed for natural hazards. For example, preattack emergency orders might direct BPS entities to increase generation reserves and/or re-dispatch resources out of least-cost operations. Other orders might be threat specific: for example, to intensify scrutiny of operational technology networks for malware and implement government-vetted counter-measures in ways that give utilities sufficient latitude to account for their unique system characteristics.

The common denominator for all such options: if the secretary issues orders for BPS entities to adopt conservative operations and adversaries decide not to strike, government and industry leaders will have no regrets about having implemented the orders.

---

<sup>123</sup> See, for example, PJM, *PJM Manual* 13, 73; Lucas, “Conservative Operations”; and SERC, *Conservative Operations Guidelines*.

However, because so many utilities already have robust plans and capabilities to protect their systems from imminent threats, close government–industry coordination will be required to ensure that emergency orders actually assist grid defense rather than function as speed bumps or useless distractions. Reliability coordinators and other grid operators serve as the pointy end of the spear for protecting grid reliability. Mandatory NERC standards require BPS entities to maintain voltage stability, automatic load shedding schemes, and contingency reserves for disturbances.<sup>124</sup> NERC standards also require transmission operators to “develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area.”<sup>125</sup> Balancing authorities have similar requirements to manage generating and demand-side resources in their service areas.<sup>126</sup> These plans are exercised, tested, and frequently updated to bolster their effectiveness for actual emergencies. While many of NERC’s mandatory standards apply when disturbances begin to occur, BPS entities are spring-loaded to implement conservative operations the moment potential hazards begin to emerge.

If major grid disruptions occur, BPS entities will not sit on their hands and wait for the president to declare a grid security emergency and the secretary to issue emergency orders. Indeed, DOE does not contemplate that they will. In the final grid security emergency rule, the department states that the declaration of a grid security emergency “does not preclude electric utilities from taking time-sensitive action to secure the safety, security, or reliability of the electric grid prior to the issuance of an emergency order.”<sup>127</sup>

DOE and its partners can design emergency orders to help supplement and support such industry-led operations. For example, government agencies may acquire highly classified indicators that an attack is imminent. Declaring a grid security emergency and issuing emergency orders for conservative operations could ensure that utilities bolster their preparedness against such attacks on a consistent, nationwide basis, including those utilities that had not yet identified a need to act. Orders to help power companies ramp up and target searches for specific types of malware could supplement utilities’ defensive operations as well. The secretary might also issue orders to ensure that such industry operations benefited from the FPA’s regulatory protections and cost-recovery provisions.

### More Disruptive Preattack Options

Many utilities are also prepared to take pre-event emergency measures that will significantly disrupt normal electric service, yet also offer benefits far beyond those that conservative operations can provide. For example, power companies can selectively halt electric service on warning of catastrophic storm surges. If seawater hits systems that are still carrying electricity, transformers and other difficult-to-replace grid components will suffer catastrophic physical damage. In 2012, weather forecasters warned that Superstorm Sandy might produce storm surges that would inundate critical substations and underground electrical equipment in lower Manhattan. Consolidated Edison’s team made the politically difficult decision to prevent such damage by preemptively cutting of power to the area. Doing so enabled much faster restoration than would have been possible if the utility had left the grid energized.<sup>128</sup> Moreover, Consolidated Edison limited the shutdown’s disruptiveness by notifying customers hours earlier that the utility might halt service and by already having plans in place to prioritize the

<sup>124</sup> See, for example, NERC, *VAR-001-4.2*; NERC, *Standard PRC-006-3*; NERC, *PRC-010-2*; and NERC, *BAL-002-2(i)*.

<sup>125</sup> NERC, *EOP-011-1*, R1.

<sup>126</sup> NERC, *EOP-011-1*, R2.

<sup>127</sup> DOE, “RIN 1901–AB40,” 1177.

<sup>128</sup> Miller, “Con Edison Shuts off Power.”



restoration of service to hospitals, water-pumping stations, and other critical facilities.<sup>129</sup>

BPS entities continue to use “shutdown on warning” as an effective tool to avoid equipment damage against severe weather and thereby shorten the duration of power outages. For example, ahead of Hurricane Harvey (2017), transmission owners and operators preemptively shut down several local load networks in a controlled fashion to prevent equipment damage and speed up restoration. Generation owners similarly chose to shut down or evacuate some generating units in the storm’s projected path.<sup>130</sup>

The grid operators who decide to execute these shutdowns are making a high-profile gamble. Based on predictions of storm surges and other weather effects, which may not turn out to be accurate, they are intentionally cutting off ongoing service to customers who would (all things being equal) likely prefer to keep their lights, elevators, and heating and air conditioning systems functioning. But the drastically shortened restoration timelines that shutdowns enable could make the gamble worth taking.

DOE and its electricity subsector partners should consider developing emergency orders that offer a similar set of risks and rewards. However, doing so will entail problems beyond those associated with protecting the grid against natural hazards. While predicting storm surges can be difficult, far greater uncertainties will surround assessments of whether an adversary will actually pull the (cyber) trigger and whether attacks are likely to cause demonstrable harm to the US economy, national security, or public health and safety. Measures developed for natural hazards may also offer uncertain benefits against imminent cyber and physical attacks. For example, further analysis will be required to determine whether and how preattack grid shutdowns might help counter specific cyber threats, including attacks that disable

protection systems to facilitate equipment-damaging power surges.

Other disruptive emergency orders could counter a broader range of threats but entail major (and perhaps insurmountable) problems for nationwide employment. The upper left-hand box in Figure 5 offers a prime example of such options: preplanned power islanding. Microgrids offer the most familiar means of establishing power islands.<sup>131</sup> A growing number of military bases, universities, and major hospitals have sufficient generation and other electric infrastructure on-site so that if adversaries black out the surrounding grid (or pose an imminent danger of doing so), those facilities can separate from the grid and operate independently as power islands.

However, microgrids do not offer “bulletproof” power resilience. Cyber adversaries are sure to treat on-base electric infrastructure, including renewable generation assets, as prime targets for advanced persistent threats. For the growing number of microgrids that rely on natural gas-fired generators, the power they provide is only as resilient as the gas transmission and distribution systems that supply them—and cyber threats to natural gas systems are rapidly escalating.<sup>132</sup> Moreover, building microgrids requires extensive investment in grid infrastructure. Investment demands will be especially heavy if installations want to serve not only the critical loads within their perimeters but also the water systems, hospitals, and other vital infrastructure in the surrounding communities where their employees live.

As an alternative to building microgrids, power companies are also analyzing ways to establish emergency power islands with less infrastructure investment. One particular option being explored by GridEx participants is to preplan to establish large

<sup>129</sup> DiSavino and Sheppard, “ConEd Cuts Power.”

<sup>130</sup> NERC, *Hurricane Harvey*, v.

<sup>131</sup> DOE’s definition of microgrids: “A microgrid is a local energy grid with control capability, which means it can disconnect from the traditional grid and operate autonomously.” “The Role of Microgrids,” DOE.

<sup>132</sup> DOE, *Quadrennial Energy Review*, 7-7; and Parfomak, *Pipelines*, 2-3.

power islands by using existing grid infrastructure within their boundaries. Utility personnel have noted that they might be able to use legacy balancing areas as a starting point to establish island boundaries. On warning of an imminent attack or under other extraordinary circumstances, utilities would separate a power island from the surrounding grid and operate independently to serve critical loads within it. In theory, if utilities can configure islands to match generation with load, and have the trained personnel and operational capabilities necessary to manage the islands and preserve their stability, preplanned islands might become a hedge against cascading failures and uncontrolled separation.

In practice, preplanned islanding will be practical only if the electricity subsector first overcomes immense (and potentially unresolvable) technical impediments to island design and operation. All of the problems of securing small-scale microgrids would need to be resolved at a larger scale for preplanned islands. Potentially significant supplementary investments in infrastructure would also be needed for many, if not all, such islands to enable them to function independently of the grid. Moreover, standing up islands would severely disrupt day-to-day service for noncritical customers and create instabilities for surrounding systems that could produce additional service disruptions. Accordingly, preplanned islanding might be considered a “huge-regrets” emergency order. If attacks failed to materialize, government leaders issuing such orders could be expected to receive a torrent of criticism for the disruptions they created.

DOE and its industry partners should also consider developing preattack emergency orders that fall between the two extremes of no-regrets options and highly disruptive measures. For example, to avoid remote execution of destructive malware on utility networks, orders might direct utilities to disconnect their systems from the internet. Utilities could also take additional measures to isolate or compartmentalize all control systems. Implementing these

measures would curtail potential attack vectors, but would do so at a price. Disconnecting from the internet would hobble wholesale market operations, disable email as a basic communications tool, affect an entity’s access to other means of communications (i.e., E-ISAC and DOE portals), impact an entity’s ability to comply with regulatory requirements, and produce other undesirable consequences. Any unexpected challenges in isolating or compartmentalizing the control systems that are critical to the functioning of the grid could also jeopardize normal service. Nevertheless, if industry and its government partners can preplan to anticipate and overcome these challenges, even highly disruptive preattack options may be useful to protect the grid from cascading failures.

## Extraordinary Measures when Attacks Are Occurring

Emergency orders when attacks are underway can help utilities prevent widespread instabilities, cascading failures, and uncontrolled separation. Under the auspices of the ESCC, utilities and their resilience partners are already developing “extraordinary measures” to operate the grid if adversaries disable or corrupt SCADA (supervisory control and data acquisition) systems, state estimators, and other operational technology hardware and software components on which utilities typically rely.<sup>133</sup> For example, the North American Transmission Forum is leading an initiative on supplemental operating strategies to help power companies manually cope with the loss of energy management systems and/or SCADA across a large geographic footprint.<sup>134</sup>

<sup>133</sup> These extraordinary measures include resorting to manual operations, engaging in planned separations, leveraging secondary and tertiary backup systems, and development of supplemental operating strategies use in “degraded states.” See “ESCC: Electricity Subsector Coordinating Council,” ESCC.

<sup>134</sup> Galloway, “Advancing Reliability and Resilience of the Grid,” 2.



These industry efforts provide a basis to develop grid security emergency orders for extraordinary measures when attacks are under way. So, too, do existing BPS emergency operating plans, capabilities, and operational requirements to manage the grid instabilities. Options for such orders vary in terms of the disruption they would inflict on normal grid operations.

Figure 5 provides an example of a low-disruption order for this phase: suspending wholesale electricity markets. In major portions of the United States, BPS entities rely on wholesale markets to buy and sell power (either to meet their immediate needs or for the next day). These entities have taken extensive measures to keep market functions separate from their operational control of the grid. Many entities also have mechanisms in place to operate when markets are temporarily suspended. Over extended periods, however, cyber attacks that corrupt or halt wholesale markets could paralyze the flow of revenue to independent generation owners and other BPS entities, undercut the valuation of power companies on Wall Street, and magnify the damage to the US economy that attacks on the grid will create.

Regional transmission organizations are proposing emergency measures to meet this challenge. For example, PJM, which purchases power and serves as the transmission operator<sup>135</sup> for the Mid-Atlantic and other US regions, has called for the development of mechanisms to permit “nonmarket” operations in extreme circumstances.<sup>136</sup> A number of options exist to provide for such operations. For example, if the secretary were to order a temporary suspension of wholesale markets, BPS entities could buy and sell

power at a fixed price predetermined by DOE.<sup>137</sup> Such measures could forestall major economic dislocations for power companies without degrading day-to-day service. Other potential high-benefit/low-disruption emergency orders, including orders for maximum power generation when attacks are under way, will also fall into this category.<sup>138</sup>

Industry and government partners will also need to develop more disruptive emergency orders that can protect grid reliability in extraordinary circumstances. One option to do so involves operating an area in a generation-deficient state for a prolonged period, supported (when practical) by power imported from neighboring regions. The top center box of Figure 5 provides another prominent example: prioritized manual load shedding. When severe events create a shortfall in the generation and transmission resources needed to serve the loads on a system, system operators help prevent grid instabilities and cascading outages by selectively shedding load and implementing rotating blackouts.<sup>139</sup>

A failure to shed load contributed to the cascading failures in the major 2003 blackout. After-action reports from that event found that if grid operators had acted quickly to drop significant amounts of customer load, lessening the burden on transmission

<sup>135</sup> The NERC glossary defines *transmission operator* as “the entity responsible for the reliability of its ‘local’ transmission system, and that operates or directs the operations of the transmission facilities.” *Transmission operator area* is defined as “the collection of Transmission assets over which the Transmission Operator is responsible for operating.” See NERC, *Glossary*.

<sup>136</sup> PJM, “Comments and Responses,” 6, 39–40.

<sup>137</sup> Alternatives proposed by PJM include cost-based compensation for power providers and direct operation of generators. PJM, “Comments and Responses,” 39.

<sup>138</sup> Maximum generation involves increasing generation “above the maximum economic level” when additional generation is needed. See PJM, *PJM Manual* 13, 35. Maximum generation orders can add much greater capacity (and bolster reserves accordingly) than pre-event conservative operations would typically provide. Such orders would also incur significantly greater costs. However, orders for maximum generation would not disrupt service to customers. On the contrary: by helping BPS entities manage fluctuating load and other instabilities, such orders could help reduce the likelihood of outages. For an example of how BPS entities have used maximum generation orders in severe weather events, see MISO, “MISO January 17–18 Maximum Generation Event Overview.”

<sup>139</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 11.

lines and thereby reducing the risk of additional lines tripping off, operators could have greatly narrowed the geographic scope of the blackout. A US–Canada task force found that “timely and sufficient action to shed load on August 14 would have prevented the spread of the blackout beyond northern Ohio.”<sup>140</sup> In some areas of New England and the Maritimes, load shedding did successfully stabilize frequency and voltage and prevented further cascading.<sup>141</sup>

Based on lessons learned from 2003 and subsequent cascading failures, NERC has established an extensive set of FERC-approved reliability standards to reduce the risk of such failures, including requirements for transmission operators to maintain and exercise plans for emergency under-voltage and under-frequency load shedding. Those standards provide a foundation for building emergency orders to reduce the risk that physical and cyber attacks will create cascading blackouts.

One way to shed load would be to order power companies to execute rotating blackouts. In such controlled outages, grid operators interrupt service on a rotating basis to sequential sets of distribution feeders for limited periods (typically twenty to thirty minutes).<sup>142</sup> Grid operators employed rotating blackouts to help protect grid reliability during the “Big Chill” that struck Texas in February 2011. Freezing temperatures caused 210 generating units within the Electric Reliability Council of Texas, Inc. (ERCOT) to fail or otherwise cease operating. To manage the resulting shortfall in available power, ERCOT’s rotating blackouts during the event affected a total of 4.4 million customers.<sup>143</sup> The temporary blackouts were no doubt disruptive. However, by reducing the risk of cascading failures, those

outages offered compelling system-wide benefits for protecting reliability.

But rotating blackouts will not offer the best option for load shedding in all grid security emergencies. In the event of a massively disruptive attack, an emergency order might require utilities to shed load without implementing rotating blackouts, because such rotating outages could introduce unacceptable reliability risks during a chaotic and rapidly changing situation. As an alternative, utilities can implement “brownouts”: that is, conduct voltage reductions to maintain a continual balance between supply and demand within a balancing area.<sup>144</sup> However, brownouts and rotating blackouts share a serious limitation: they affect all customers equally. But not all customers will be equally important in a grid security emergency. DOE and industry will need orders and implementation plans for manual, prioritized load shedding, so utilities can focus on sustaining power flows to hospitals and other critical loads while also reducing the risk of cascading power failures. NERC already requires BPS entities to have plans for both automatic and manual load shedding.<sup>145</sup> Utilities and DOE should use these requirements as the starting point to design emergency orders for extraordinary measures that would supplement what BPS entities are already prepared to do to if major instabilities occur.

## Emergency Orders to Support Power Restoration

The rightmost column in Figure 5 provides the third category for emergency orders: those that can help grid owners and operators restore power after widespread

<sup>140</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 147.

<sup>141</sup> U.S.-Canada Power System Outage Task Force, *Final Report on Blackout*, 77.

<sup>142</sup> NERC, *Reliability Terminology*, 1.

<sup>143</sup> FERC and NERC, *Restoration and Recovery Plans*, 61.

<sup>144</sup> NERC, *Reliability Terminology*.

<sup>145</sup> NERC standards currently emphasize automatic load shedding to protect grid reliability. See NERC, *Standard PRC-006-3*; and NERC, *PRC-010-2*. However, NERC standards for emergency operations include provisions for manual load shedding, which can be the basis for further progress in designing emergency orders to prevent or mitigate cascading failures. See NERC, *EOP-011-1*.

outages occur. In past cascading failures of the US electric system, including the 2003 blackout, power companies have been able to rapidly restore power in a few days (and in some cases much less time) because transformers and other equipment survived undamaged. That lack of damage reflects a key design feature of the grid. Generators, transmission lines, and other system components are designed to trip offline when instabilities occur, thereby protecting them from damaging power surges—and leaving them available to help rapidly reestablish the flow of power.<sup>146</sup> However, if cyber or physical attacks destroy critical system components, requirements to repair or replace such assets could greatly lengthen and complicate the restoration of service. Emergency orders can support restoration operations and better align them with national-level priorities.

Emergency orders for the restoration phase can also account for the risk that adversaries may continue their attacks as power companies begin to restore service. It would be foolish to assume that adversaries will launch only a single strike and then sit back to admire their handiwork. Unless the regional crisis or other confrontation that triggered the attack has been resolved, we should expect adversaries to continue their efforts to deny electric service to US military bases and other vital facilities and to seek to corrode the ability and willingness of the United States to prevail in the conflict. Attacks targeting power restoration operations can help adversaries achieve those goals by further lengthening the duration of blackouts, especially as public and private sector emergency power systems fail from extended use and shortfalls in fuel resupply. Risks of reattack should help drive the design of restoration-phase emergency orders.

Advanced persistent threats hidden in utility networks will pose especially significant challenges for restoration. This malware may enable adversaries to conduct recurring attacks based on timing or network

conditions. Unless utilities thoroughly eradicate such malware, repeated outages could impede restoration operations and put the grid at sustained risk of cascading failures.<sup>147</sup> Physical attacks against restoration personnel and replacement equipment in transit would pose additional problems. Grid security emergency orders can help utilities restore electric service even if they remain “under fire” from cyber and kinetic weapons.

Such orders will differ in the degree to which they could alter existing utility plans to restore power. In the lower right-hand box, support for transformer transportation offers an option that would create little or no disruption to industry-driven restoration operations. The electricity subsector has increasingly detailed and well-exercised plans in place to move spare transformers (via specialized railcars, heavy-haul trucks, and barges) from where power companies store them to where they are needed as replacements.<sup>148</sup> Subsequent portions of this report examine how DOE could collaborate with other federal agencies and state and local officials to waive transportation regulations and bolster security support for such operations. The secretary could also issue orders for prioritized restoration to speed the repair of electric systems that serve major hospitals, military bases, ports, and other vital facilities. Power companies already have their own plans that prioritize restoration for many of these prioritized customers. Emergency orders can help incorporate other national security-related assets that utility plans do not typically include, such as components of the defense industrial base essential for resupplying US forces abroad.

DOE and its industry partners should also create template emergency orders for in extremis restoration operations that would more sharply depart from existing industry plans and procedures. The upper right-hand box of Figure 5 offers an example

<sup>146</sup> NERC System Protection and Control Subcommittee, *Reliability Fundamentals of System Protection*, 1.

<sup>147</sup> Homeland Security Advisory Council, *Final Report*, 7.

<sup>148</sup> DOE, *Strategic Transformer Reserve*, 12–13.

of one such option. If adversaries damage or destroy an extraordinarily large number of transformers, the secretary might order utilities to remove surviving in-service transformers in the same voltage class from their substation and transport them to serve vital national security facilities in the National Capital Region or other areas. Orders of this kind could create severe disruptions in existing service. They might even impede system restoration if utilities and their government partners have not adequately prepared to account for challenges regarding transformers' technical specifications and the BPS's overall configuration. However, if these challenges can be addressed, the benefits might be greater still for helping the United States defeat its adversaries.

Other in extremis orders could help utilities operate the grid if equipment damage is so extensive (or reattacks are so effective) that full system restoration will require many weeks or even months. The FERC/NERC study on severe impact resilience (May 2012) found that coordinated cyber and physical attacks may force the grid into a "new normal" state of "degraded planning and operating conditions" that could last for months or years, including reduced generation and transmission resources and planned and unplanned rotating blackouts.<sup>149</sup> DOE and power companies should consider how emergency orders and supporting regulatory waivers might help electric utilities serve priority loads and accelerate restoration under new normal conditions.

One option to do so is to preplan for the waiver of selected reliability standards. The *Severe Impact Resilience* study recognized that catastrophic events could "put entities in a position where they cannot comply with all standards." However, in part due to the difficulty of predicting the circumstances that entities will face, the study recommended against preplanning for waivers. Instead, the study proposed relying on entities to "do the right thing" for reliability

and public safety" and self-report violations as circumstances permit.<sup>150</sup>

NERC should reconsider this conclusion in light of the secretary's new grid security emergency authorities and the waiver provisions they entail. FERC, NERC, and their industry and government partners should identify specific regulatory waivers and related measures that could provide the basis for utilities' contingency planning for new normal operations.

One such option lies in reliability standards for managing unforeseen contingencies. Currently, NERC standards require BPS entities to operate in an N-1 state: that is, they must be able to sustain service even if they suffer the most severe single contingency (such as the loss of a single critical line, transformer, or generator) possible in their system.<sup>151</sup> Operators may be required to shed load prior to any contingency to maintain the N-1 state. These requirements apply during normal day-to-day operations as well as during system restoration.

Returning to an N-1 state in the face of coordinated cyber and physical attacks is likely to be a lengthy process involving the re-dispatch of generation, the replacement of damaged or destroyed equipment, and partial system reconstitution. To help enable utilities to serve critical facilities during such sustained events, the secretary might issue emergency orders that explicitly allow utilities to function in an N-0 operating state (as long as doing so did not risk causing cascading failures or equipment damage).<sup>152</sup>

Issuing such orders could entail important benefits. Operating at N-0 would give utilities greater operating flexibility and ensure that entities can continue to serve as much load as possible during a grid security

<sup>149</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 14, 16.

<sup>150</sup> Severe Impact Resilience Task Force, *Severe Impact Resilience*, 17.

<sup>151</sup> NERC, *BAL-002-2(i)*, requirement R2; NERC, *TOP-001-3*, R12 and R14; and NERC, *IRO-008-2*, R5 and R6.

<sup>152</sup> For N-0, all elements must be within thermal and voltage limits prior to any contingency.



emergency, including military installations and other priority customers. Unlike under N-1 operations, entities would be required to shed load only prior to any contingency for the most severe single contingencies if any of those single contingencies would cause cascading failures, or after a contingency that required load shedding to eliminate overloads or low voltage.

But operating at N-0 would also entail significant risks. N-1 standards exist for compelling reasons: they help protect grid reliability against severe contingencies. Deviating from N-1 requirements will create greater risks of causing further blackouts in new normal conditions. Moreover, N-0 operations would require even greater coordination among BPS entities (including reliability coordinators, transmission owners, and local control centers), as a single outage could result in equipment overloads or voltage violations and require extraordinary mitigation measures. Accordingly, this option will be feasible only if DOE partners with FERC, NERC, and entities to fully understand and mitigate such risks, as well as maximize the potential benefits of N-0 operations for serving critical national security-related loads.

## Additional Emergency Order Design Parameters and Supporting Initiatives

Adversaries will attempt to black out the US grid to achieve their broader political, economic, and military objectives in a conflict. Government agencies and the electricity subsector should design emergency orders to help prevent attackers from accomplishing their objectives, and—ideally—to help deter them from attacking at all.

However, deterring and defeating attacks on the grid will require resilience improvements beyond the electricity subsector. Attackers may simultaneously strike electric and communications systems to both disrupt the grid and impede the issuance and

implementation of emergency orders. Adversaries may also seek to incite public panic through social media and other information warfare operations to advance their broader political objectives. Countering such efforts will require unprecedented collaboration among utilities, government agencies, media, and the broader telecommunications sector.

Designing and implementing emergency orders to blunt attacks by Russia, China, and other potential high-capability adversaries will place extraordinary burdens on electric utilities—burdens that few ratepayers and utility investors will be eager to bear on their own. To help power companies meet these challenges, it will be essential to fully leverage the regulatory waiver and cost-recovery provisions of the FPA, and examine whether Congress should expand these provisions as threats continue to intensify.

## Deterring and Defeating US Adversaries

The US *National Security Strategy* emphasizes that cyber threats to US critical infrastructure are becoming increasingly severe. In particular, the strategy notes that cyber weapons “enable adversaries to attempt strategic attacks against the United States—without resorting to nuclear weapons—in ways that could cripple our economy and our ability to deploy our military forces.”<sup>153</sup> Pairing cyber attacks with coordinated physical strikes against transformers and other critical grid infrastructure would exacerbate these disruptive effects.

The strategy identifies two primary means for deterring catastrophic attacks, both of which can be supported by emergency orders and implementation plans:

- (1) Convince adversaries that they will suffer “swift and costly consequences” if they strike the grid or other US targets, and that the United States “can and will defeat them” if deterrence fails.<sup>154</sup>

<sup>153</sup> White House, *National Security Strategy*, 13, 28.

<sup>154</sup> White House, *National Security Strategy*, 28.



- (2) Strengthen infrastructure resilience to create “doubt in our adversaries that they can achieve their objectives” if they do attack (i.e., deterrence by denial).<sup>155</sup>

### **Deterrence through Cost Imposition: Protecting Defense Critical Electric Infrastructure**

In amending the FPA, Congress placed a particular emphasis on the need to protect the reliability of defense critical electric infrastructure (i.e., grid components that serve military bases and other facilities “critical to the defense of the United States” and vulnerable to the disruption of grid-provided electricity).<sup>156</sup> Emergency orders to protect such infrastructure can help ensure that US bases have the power they need to respond to attackers. But prioritizing defense installations for support in grid security emergencies will require deeper analysis of US deterrence requirements, given DOD’s growing dependence on civilian assets and functions to execute defense missions. Deterrence by cost imposition will also depend on convincing potential adversaries that the United States will be able to identify them as the perpetrators of attacks on the grid. DOE and its industry partners should explore how emergency orders can facilitate attack attribution, as well as provide broader support for the credibility of the US deterrence posture.

A relatively small number of military bases are responsible for inflicting unacceptable costs on potential adversaries. The US Defense Science

Board Task Force on Cyber Deterrence (2017) recommended that as a top priority, DOD should reinforce the cyber resilience of US strike systems (cyber, nuclear, and nonnuclear) and supporting infrastructure to ensure “that the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attacks.”<sup>157</sup> Initiatives to develop emergency orders and contingency plans should adopt a similar focus. Industry and government partners should immediately prioritize the protection of defense critical electric infrastructure that supports installations and functions on which US strike systems rely and ensure that they have reliable power even in extended conflicts.

Emergency orders can also help achieve a closely related goal established by the *National Security Strategy*. The strategy emphasizes that “we must convince adversaries that we can and will defeat them—not just punish them if they attack the United States.”<sup>158</sup> Defeating adversaries in regional contingencies in the South China Sea, the Baltics, or other potential conflict zones will place special burdens on US grid resilience. US capabilities to conduct operations abroad are increasingly dependent on domestic military and civilian assets. In particular, a vast array of US defense installations, as well as civilian-operated ports and transportation infrastructure, are required to deploy, operate, and sustain US power projection forces for regional conflicts.

This dependence makes the grid a prime target for attack. The *DOD Mission Assurance Strategy* notes that adversaries may seek to disrupt power projection capabilities by attacking the domestic infrastructure systems on which they depend. In particular, the strategy warns that “potential adversaries are seeking asymmetric means to cripple our force projection, warfighting, and sustainment capabilities by targeting

---

<sup>155</sup> White House, *National Security Strategy*, 13, 28. The literature on security studies defines deterrence by denial in a variety of ways. This report follows the definition used in the *National Security Strategy*, which is consistent with the definition employed in the Obama administration’s deterrence policies. See Lynn, “Defending a New Domain.” For broader studies of deterrence by denial, and critiques of the way in which the strategy employs the term, see Fischerkeller and Harknett, “Deterrence Is Not a Credible Strategy”; Mitchell, “Case for Deterrence by Denial”; Gerson, “Conventional Deterrence,” 40; and Nye, “Deterrence and Dissuasion,” 56–58.

<sup>156</sup> 16 U.S.C. § 8240–1, (a)(4).

---

<sup>157</sup> Miller and Gosler, “Memorandum.” See also pp. 3, 6–7, 11–12, and 17–18 of the report.

<sup>158</sup> White House, *National Security Strategy*, 28.

critical defense and supporting civilian capabilities and assets,” including the US power grid.<sup>159</sup>

Ensuring the availability of resilient power for ports and other civilian assets essential for power projection will require emergency orders to serve an expanded set of customers, far beyond those responsible for strike operations. These orders will also need to encompass a much larger array of defense critical electric infrastructure owners and operators.

Electric companies and defense installations are already making infrastructure investments to counter this asymmetric threat. Building redundant power feeds from separate high-voltage transmission substations to serve defense installations provides a valuable means of strengthening resilience against physical attacks.<sup>160</sup> Many military bases are also adding emergency power generators to serve critical loads if adversaries disrupt grid-provided power.<sup>161</sup> Utilities and DOD are also beginning to construct microgrids on military bases in Hawaii, Michigan, and other states that can enable bases to operate as power islands independent of the surrounding grid.<sup>162</sup>

While valuable, these initiatives do not eliminate the need to develop national defense-oriented emergency orders. Redundant power feeds are not practical for many remote military bases and will not necessarily provide resilience against cyber attacks (since even redundant feeds may share common cyber vulnerabilities). Emergency generators will break down in long-duration outages. Moreover, resupplying them with fuel will become increasingly difficult at installations that lack massive storage

tanks. Large-scale microgrids for islanded operations can provide more resilient power. DOD and power companies should partner to improve policies and funding mechanisms to facilitate their construction and scale them to serve infrastructure loads outside the base that are essential for on-base operations. Yet, even with such improvements, it will take many years to construct microgrids at all the installations essential for war fighting and deterrence. Still greater time and infrastructure spending would be required to enable islanded operation by the civilian assets on which DOD depends, including the intermodal transportation systems that help deploy and sustain US forces abroad.

DOE and its industry partners can design emergency orders to support US deterrence credibility and power projection capabilities far more quickly and with less infrastructure investment. However, for utilities to implement these orders, they must first know which customers are of the highest priority for sustaining and restoring service when enemies strike. Section 215A of the FPA provides the ideal starting point develop and share such data. The act requires the secretary of energy, in consultation with other federal agencies and grid owners and operators, to identify and designate “critical defense facilities” in the forty-eight contiguous states and the District of Columbia that are “(1) critical to the defense of the United States; and (2) vulnerable to a disruption of electric energy provided to such facility by an external provider.”<sup>163</sup> Congress’s definition of defense critical electric infrastructure also helps guide implementation of that requirement. Such assets include “any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary [of Energy]” as a critical defense facility, “but is not owned or operated by the owner or operator of such facility.”<sup>164</sup>

<sup>159</sup> DOD, *Mission Assurance Strategy*, 1.

<sup>160</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 39.

<sup>161</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 40.

<sup>162</sup> ASD(EI&E), *AEMR Report Fiscal Year 2016*, 39. See also Van Broekhoven et al., *Microgrid Study*; and Marqusee, Schultz, and Robyn, *Power Begins at Home*, 13–15. A number of “islandable” microgrid projects are under way at military bases, including installations in Hawaii, California, Georgia, California, New York, and Illinois. See McGhee, “EEI Executive Advisory Committee,” 4; and Kaften, “DoD Tests Energy Continuity.”

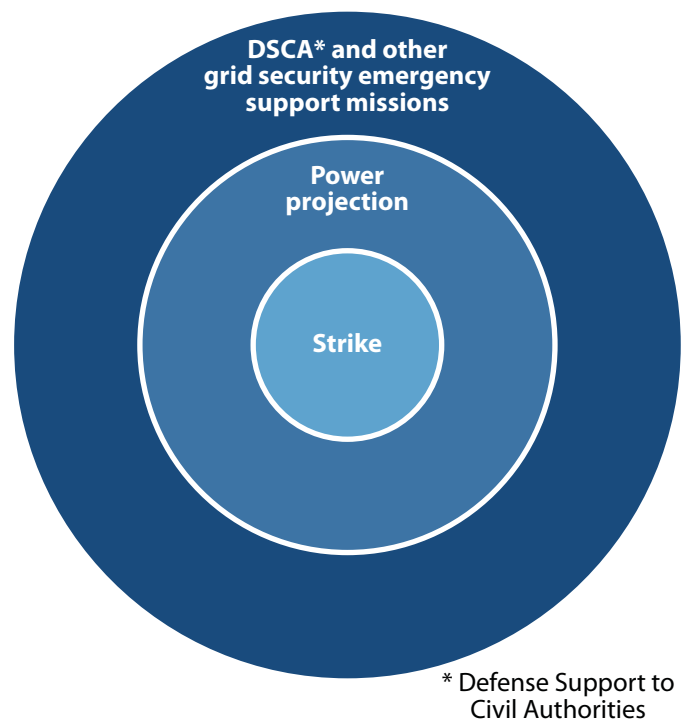
<sup>163</sup> 16 U.S.C. § 824o–1, (c).

<sup>164</sup> 16 U.S.C. § 824o–1, (a)(4).

DOE is already working with DOD to identify defense critical electric infrastructure and the installations this infrastructure serves. DOD has a well-established, continuously updated list of critical military bases and other DOD assets to support this identification process.<sup>165</sup> However, deterrence and power projection will also depend on sustaining electric service to a diverse array of ports, transportation systems, and other civilian-owned infrastructure. Figure 6 illustrates how DOE, DOD, and their partners might categorize all such defense-related assets and the defense critical electric infrastructure that grid security emergency orders should help protect.

At the innermost core lie those installations and supporting infrastructure capable of inflicting swift and costly consequences on attackers. These strike assets are small in number but absolutely vital. Protecting the reliability of the defense critical electric infrastructure on which they depend should be the top nationwide priority for developing emergency orders and company-specific implementation plans.

The second circle encompasses the force projection assets and civilian-owned infrastructure essential for deploying and sustaining these assets abroad, and for convincing adversaries that we can defeat them in regional conflicts that could precipitate attacks on the US grid. That circle encompasses far more bases than necessary for strike options, along with a large number of ports, transportation systems, and other civilian assets that support regional operations. DOD is in the process of identifying the specific facilities and supporting infrastructure that are required to help execute operational plans around the globe.<sup>166</sup> The department also has well-established criteria and assessment methods to prioritize these supporting assets for risk mitigation.<sup>167</sup> DOD and DOE should use these tools to identify the broader set of defense critical electric infrastructure needed for deterrence



**Figure 6. Categories for Protecting Defense Critical Electric Infrastructure**

and to help power companies preplan to support critical assets within their service footprints.

The third circle includes the still larger array of defense installations, including National Guard bases, which would be essential for providing defense support to civil authorities if disruptions of the grid jeopardize public health and safety.<sup>168</sup> During Hurricane Maria (2017), Superstorm Sandy (2012), and other severe natural disasters, tens of thousands of military personnel deployed to help civilian agencies save and sustain lives. Military bases also help utilities restore power by providing staging support (food, lodging, etc.) to grid repair crews, clearing roads so crews can access damaged equipment, and delivering other assistance. Protecting or rapidly restoring the reliability of the defense critical electric infrastructure that supports

<sup>165</sup> See DOD, *Manual 3020.45*; and DOD, *Directive 3020.40*.

<sup>166</sup> DOD, *Directive 3020.40*.

<sup>167</sup> DOD, *Manual 3020.45*.

<sup>168</sup> Of course, many National Guard installations that could conduct defense support operations may also be responsible for assisting war fighting operations abroad, and would therefore fall within the second circle as well.

these defense-support-to-civil-authorities functions will help prevent adversaries from achieving the broader political effects they may seek by cutting off power to the American public.<sup>169</sup>

Building preparedness for grid security emergencies can also help meet an underlying challenge for deterrence: attack attribution. To convince foreign leaders that they will suffer swift and costly consequences if they strike the grid, those leaders must first believe that the United States will be able to identify them as the attackers.<sup>170</sup> The Federal Bureau of Investigation (FBI) and other federal agencies are improving their attribution capabilities.<sup>171</sup> US agencies also devote massive resources to human and technical intelligence collection on potential adversaries, which could further assist attack attribution.<sup>172</sup> Nevertheless, adversaries may seek to strike in ways that complicate attack forensics by employing wiper tools and using other tactics, techniques, and procedures to cover their tracks.<sup>173</sup>

Emergency orders can help defeat adversaries' efforts to evade attribution. By refining the FPA's information sharing mechanisms and building them into emergency orders, utilities and their government partners can strengthen their ability to share malware samples and other information on threat signatures.<sup>174</sup> New technologies can bolster such collaboration. For

example, the Containerized Application Security for Industrial Control Systems project is designed to help grid operators isolate and capture malware on their systems, enabling samples to be shared with government agencies while still preventing that malware from disrupting system operations.<sup>175</sup>

Developing emergency orders and implementation plans to defend the grid can also provide broader support for attribution. James Miller notes that "while cyber hardening of US critical infrastructure will never be good enough to prevent a Russia or China from being able to threaten a major attack, it can cause them to have to be 'noisier' to do so, thereby boosting our confidence in attribution."<sup>176</sup> Emergency measures to protect grid reliability can complicate attack planning and, ideally, drive adversaries to strike in ways that will make them easier to identify.

### **Deterrence by Denial: Protecting Critical Electric Infrastructure**

Convincing adversaries that they will suffer unacceptable costs if they strike the grid is only one means of deterring such attacks. Another means is to reduce the benefits that adversaries expect to achieve by attacking. In classical deterrence theory, both factors combine to influence an adversary's decision on whether to strike. As Joseph Nye Jr. puts it, "deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit."<sup>177</sup>

The *National Security Strategy* calls for measures that can prevent attackers from achieving the goals they seek and thereby strengthen deterrence by denial. The strategy states that "we must ensure the ability to deter enemies by denial, convincing them that they cannot accomplish their objectives through the use of

<sup>169</sup> Countering such adversary efforts will also require protecting electric service to financial institutions, regional hospitals, and other civilian assets essential to the US economy and public health and safety. The next section of the report examines these requirements and their implications for deterrence and emergency order design.

<sup>170</sup> On the tasks that attribution comprises, see Lin, "Escalation Dynamics," 49–50.

<sup>171</sup> Smith, "Roles and Responsibilities." See also Newman, "Hacker Lexicon."

<sup>172</sup> Miller, "Cyber Deterrence."

<sup>173</sup> Newman, "Hacker Lexicon."

<sup>174</sup> See 16 U.S.C. § 824a–1, (d). Later sections of this report provide a more detailed assessment of provisions for improved information sharing.

<sup>175</sup> "Sandia's Grid Modernization Program Newsletter," Sandia National Laboratories.

<sup>176</sup> Miller, "Cyber Deterrence."

<sup>177</sup> Nye, "Deterrence and Dissuasion," 45.



force or other forms of aggression.”<sup>178</sup> Ensuring that the grid and other infrastructure sectors can survive attacks and rapidly recover from service interruptions plays an especially important role in the administration’s deterrence posture. The strategy notes that “a stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives.”<sup>179</sup> More recent statements of administration policy also note that deterrence by denial “must be foundational to the U.S. deterrence approach,” and that US efforts must continue “to deny adversaries the benefits of their malicious cyber activities.”<sup>180</sup>

Emergency orders and implementation plans may be able reduce the benefits that adversaries expect to achieve by attacking the grid. Preattack orders to bolster grid defenses can impede adversary efforts to disrupt grid reliability. Once attacks are under way, orders for prioritized load shedding and other extraordinary measures can help limit the damage the adversaries may hope to inflict on financial institutions, hospitals, and other electricity-dependent facilities. Orders that accelerate power restoration to these critical facilities may also reduce the effects of an attack, and thereby strengthen deterrence by denial.

The FPA is ready-made to support such improvements. In addition to protecting defense critical electric infrastructure, and thereby assisting deterrence through cost imposition, the act also authorizes orders to protect a much broader portion of the grid: critical electric infrastructure. Such infrastructure comprises grid systems or assets whose incapacity or destruction would “negatively affect national security, economic security, public health and safety, or any combination of such matters.”<sup>181</sup> Orders to help utilities defend critical electric infrastructure can reinforce deterrence by denial—and, if deter-

rence fails, reduce the devastation that adversaries will create.

However, developing and implementing such orders will entail major challenges. Some deterrence theorists doubt whether deterrence by denial is practical in cyberspace, in part because offensive capabilities are so much stronger than cyber defenses. The conclusion of this report will examine those arguments and explore broader opportunities to bolster deterrence and help the United States defeat our adversaries if conflicts nevertheless occur. First, however, DOE and its partners will need to overcome two impediments to protecting critical electric infrastructure: determining which specific facilities and functions are truly critical, and securely sharing that information with utilities so they can refine their operational plans for grid security emergencies.

### **Building a “Section 9+ List:” Prioritizing Infrastructure for Sustainment and Restoration**

Identifying and prioritizing critical electric infrastructure will be far more difficult than doing so for defense critical electric infrastructure. If adversaries create cascading blackouts across one or more interconnections, the disruption of many thousands of civilian-owned facilities could negatively affect national security, the US economy, and public health and safety. Utilities cannot possibly prioritize the flow of power to all such facilities. Government agencies and their private sector partners will need to determine which specific customers (and the critical electric infrastructure that serves them) are most vital to the nation and must continue to receive power if widespread instabilities occur.

Executive Order 13636 (February 2013) provides an existing methodological starting point to create a comprehensive prioritization list. Section 9 of that order requires the secretary of homeland security to maintain a list of critical infrastructure whose disruption in a cybersecurity incident “could reasonably result in catastrophic regional or national effects on public health or safety, economic security,

<sup>178</sup> White House, *National Security Strategy*, 28.

<sup>179</sup> White House, *National Security Strategy*, 13.

<sup>180</sup> DOS, *Recommendations*, 2.

<sup>181</sup> 16 U.S.C. § 824o–1, (a)(2).



or national security.”<sup>182</sup> That standard—catastrophic damage—provides a useful criterion to identify the highest-priority assets and associated critical electric infrastructure for protection by emergency orders in grid security emergencies. Over time, orders and contingency plans could gradually encompass less-critical facilities and grid infrastructure.

Of course, the section 9 methodology and subsequent list were never intended to support the implementation of section 215A of the FPA. As a result, the section 9 methodology falls short of meeting all the requirements for supporting emergency order design. One gap lies in the threats that drive the selection of critical assets. Section 9 focuses exclusively on infrastructure at risk from cyber attacks. The FPA provides for the development of emergency orders to protect electric service against other hazards as well, including electromagnetic threats and physical attacks on electric systems. Executive Order 13636’s section 9 requirements also create a “corporate”-level list that is not broken down into the key assets within those corporations (i.e., facilities, systems, and nodes). More fine-grained data and analysis will be required to identify facilities for which sustained electric service will be most crucial. Efforts to prioritize grid service will also need to account for the increasingly complex interdependencies between US infrastructure sectors.<sup>183</sup>

Despite these shortfalls, Executive Order 13636’s methodology can provide a valuable starting point for identifying the most vital critical electric infrastructure and supporting assets. DOE and its industry partners should leverage that methodology to create a “section 9+” list, tailored to fulfill FPA emergency order requirements. Other government initiatives to prioritize critical infrastructure could

also make valuable contributions to the list and overall prioritization effort. For example, DHS’s May 2018 cyber strategy emphasizes the importance of “identifying the most critical [federal] systems and prioritizing protections around those systems.”<sup>184</sup> A number of other initiatives could provide significant value as well.<sup>185</sup> Building a section 9+ list would also benefit from the inclusion of input from cleared state regulators and homeland security and emergency management officials.

DHS’s National Risk Management Center can help integrate these sources of data and develop a comprehensive, cross-sector basis for prioritizing the sustainment and restoration of power to critical facilities. Government agencies within the center will collaborate with the private sector to “identify, assess, and prioritize efforts to reduce risks to national critical functions, which enable national and economic security.” One immediate task will be to “help define what is truly critical.”<sup>186</sup> As this work

<sup>184</sup> DHS, *Cybersecurity Strategy*, 8.

<sup>185</sup> There are numerous programs that DOE and its partners could leverage to build the section 9+ list. DHS’s National Critical Infrastructure Prioritization Program aims to identify “nationally significant assets, systems, and networks which, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, and/or widespread and long-term impacts to national well-being and governance.” See DHS, *NIPP 2013*, 17. The NIPP also calls for an effort to analyze cross-sector vulnerabilities and consequences to facilitate an infrastructure prioritization effort that focuses on “lifeline functions and the resilience of global supply chains during potentially high-consequence incidents, given their importance to public health, welfare, and economic activity” (p. 24). Despite its focus on terrorist threats, *Homeland Security Presidential Directive 7* also requires the secretary of homeland security to identify and prioritize systems and assets that, if destroyed or disrupted could cause catastrophic effects to public health and safety, the economy, or national security. Additionally, the amended Homeland Security Act requires the creation of a national database of assets and systems, the “loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States” and lower jurisdictions. The national-level priorities on this list could also be helpful. 6 U.S.C. § 124l, (a)(2).

<sup>186</sup> “National Risk Management Center Fact Sheet,” DHS.

<sup>182</sup> Obama, *Executive Order—Improving Critical Infrastructure Cybersecurity*.

<sup>183</sup> For methodologies and data-gathering strategies to assess cross-sector interdependencies, see EIS Council, *E-PRO Handbook III*; and Homeland Security Advisory Council, *Final Report*.

goes forward, the center's efforts could contribute to the development of a section 9+ list that will be essential for grid security emergency preparedness.

### **Sharing the Section 9+ List and Protecting Critical Electric Infrastructure Information**

In addition to identifying assets most in need of power, it will also be essential to share that data with the utilities responsible for providing prioritized service. Current section 9 guidance lacks the provisions for information sharing required to develop and implement emergency orders. Most importantly, while the federal government tells grid owners and operators if they are on the section 9 list, it rarely informs them about the section 9 assets in other infrastructure sectors (communications nodes, transportation systems, etc.) that lie within their service areas. Sharing that information will be essential to designing emergency orders and implementation plans that can protect power to essential facilities in other industries.

Information sharing between industry and government also faces obstacles in the other direction. While infrastructure owners and operators have the most recent and accurate data on their own system configurations and cross-sector dependencies, concerns over sharing business-sensitive information and other factors limit their willingness to share such data with government partners. Public sector leaders will need to reinforce their industry counterparts' confidence that government agencies will not use company-provided information for regulatory compliance, antitrust, or other purposes not explicitly approved through industry-government dialogue.

However, creating a baseline list that accurately reflects interdependencies across all sectors will be only the first challenge. Still more difficult will be ensuring that critical companies provide the data necessary to update that list on an ongoing basis. Even small changes to system configurations or supply chains in one industry can produce unintended and unforeseen effects on overall system resilience. Private

companies will need to help government agencies modify the section 9+ list as they reconfigure their operations and create new dependencies on outside service and product providers.

Securing and limiting the distribution of this classified data will also be a prerequisite for countering potential attacks. If adversaries acquired the section 9+ list, it would provide a roadmap that they could use to maximize their devastation of US critical infrastructure. However, measures to protect this data must be complemented by improved mechanisms to provide sensitive information to industry personnel who have the requisite security clearances.

Section 215A of the FPA offers a starting point to meet these requirements. The FPA provides for the sharing of critical electric infrastructure information, defined as information generated by FERC or other federal agencies related to identified (or proposed) critical electric infrastructure "that is designated as critical electric infrastructure information by the Commission or the Secretary" or that qualifies under FERC's critical energy infrastructure information scheme.<sup>187</sup> The FAST Act amendments directed FERC to facilitate the voluntary sharing of such information "with, between, and by" BPS entities and their government partners.<sup>188</sup> The amendments also require FERC to create criteria and procedures to designate certain information as critical and prohibit unauthorized disclosure of that information.<sup>189</sup> To help meet these requirements, FERC incorporated and is building on its well-established mechanisms to protect critical energy infrastructure information.<sup>190</sup>

---

<sup>187</sup> The definition excludes classified national security information. 16 U.S.C. § 824o-1, (a)(3).

<sup>188</sup> This includes NERC, the E-ISAC, regional entities, and "other entities determined appropriate by the Commission." See 16 U.S.C. § 824o-1, (d)(2)(D).

<sup>189</sup> 16 U.S.C. § 824o-1, (d)(2).

<sup>190</sup> FERC, *Regulations Implementing FAST Act Section 61003* (Order No. 833), 157 FERC ¶ 61,123, 13. See also FERC,

Other initiatives are also under way to provide for the protected data sharing essential for preplanning grid security emergency operations. DOE is working with the E-ISAC to develop mechanisms to facilitate the distribution of data to utilities that own and operate assets identified as defense critical electric infrastructure. Going forward, DOE, FERC, and their industry partners should refine their equivalent mechanisms to securely distribute data on critical electric infrastructure and the water systems, communications centers, and other essential non-defense assets that must continue to function in grid security emergencies.

## Communications Requirements for Issuing and Employing Emergency Orders

Over the past few decades, power companies have developed immense expertise in dealing with the communications challenges posed by hurricanes and other natural hazards. They have acquired survivable, redundant communications systems that enable them to conduct emergency operations when cell phones and other normal means of communication fail. These systems often provide connectivity with neighboring BPS entities and, to an increasing extent, entities that are farther away. Under the ESCC, industry has also built an extensive set of playbooks to help companies decide what to tell customers about an incident and to unify messaging between government officials and industry representatives on estimated times of restoration and other critical public affairs issues.

Power companies and their DOE partners are now leveraging these communications plans and capabilities to prepare for cyber and physical attacks on the grid. Preparedness for grid security emergencies will require additional progress in four areas: (1) refining consultative mechanisms and protocols for the sequential (though potentially overlapping) phases of such emergencies; (2) ensuring that communications

systems can survive adversaries' attacks; (3) authenticating emergency orders and protecting the security of sensitive data; and (4) determining what to say to the US public and accounting for the risk that adversaries will conduct information warfare operations to intensify panic and incite disorder.

## Initial Consultations and Sustained Communications

As with the phases of grid security emergency declarations, the issuance and implementation of emergency orders will also fall into sequential stages, each of which will entail different communications requirements and challenges. Preattack consultations constitute the initial stage. As noted above, the FPA specifies that before the secretary issues emergency orders, DOE will consult with power companies and other BPS stakeholders "to the extent practicable . . . regarding implementation of such emergency measures."<sup>191</sup> This report recommends that federal officials also consult with BPS entities prior to declaring a grid security emergency, since they may have valuable data and expertise to support such a determination.

The grid security emergency rule clarifies how DOE's Office of Electricity Delivery and Energy Reliability will consult on emergency orders.<sup>192</sup> The rule states that, if practicable, the E-ISAC is one of the organizations the secretary will consult. Such consultations will be particularly useful for sharing data (including classified data) on attacks that are imminent or under way. The rule also notes that DOE will consult with the ESCC. The ESCC will provide an especially valuable source of industry perspectives on grid security emergency declarations and emergency orders because it represents all components of the electricity subsector and has extensive experience in coordinating the industry's incident response operations. In addition, the rule states that "efforts

*Regulations Implementing FAST Act Section 61003* (Order No. 833-A), 163 FERC ¶ 61,125; and 18 CFR 388.113.

<sup>191</sup> DOE, "RIN 1901-AB40," 1774.

<sup>192</sup> DOE, "RIN 1901-AB40," 1181.

will be made” to consult with NERC, regional entities, “owners, users, or operators” of critical and defense critical electric infrastructure (including regional transmission operators), appropriate federal and state agencies, and other grid reliability stakeholders.

Issuing emergency orders constitutes the second stage. DOE’s grid security emergency rule states that the department will “communicate the contents of an emergency order to the entities subject to the order, utilizing the most expedient form or forms of communication under the circumstances.”<sup>193</sup> The E-ISAC will likely play a critical role in such communications, since it maintains a detailed, continuously updated list of all BPS owners, operators, and registered users (distribution entities). DOE has also emphasized its intention to use existing protocols and mechanisms for such communications, including the NERC alert system, E-ISAC notification mechanisms, and the ESCC communications coordination process.<sup>194</sup> As long as these mechanisms can be hardened as necessary to survive adversaries’ attacks, leveraging them for grid security emergencies will be much more efficient than creating a separate, unfamiliar system for communicating emergency orders.

The next stage of communications will be to coordinate operations as BPS entities implement emergency orders. Attacks on the grid are unlikely to be “one and done.” As adversaries continue to try to destabilize the grid, and power companies respond with emergency operations to protect and restore electric system reliability, sustained communications between power companies and DOE will be essential to maintain situational awareness and assess potential requirements for additional orders and response activities—potentially on a nationwide basis.

Reliability coordinators will be a critical touchpoint between DOE and individual BPS entities, serving as a focal point between DOE (and other government

leaders) and the power companies that are in their purview. This positioning makes them well suited to communicate secretary-issued orders to individual utilities. Moreover, given reliability coordinators’ responsibilities and authorities to help maintain grid reliability when incidents occur, they will also be ideally positioned to understand how grid security emergency orders should supplement BPS emergency operations that are already under way.

Sustained communications will also be necessary to meet an additional FPA requirement: responding to DOE requests for information on the implementation of emergency orders. The grid security emergency rule specifies that “beginning at the time the Secretary issues an emergency order, the Department may, at the discretion of the Secretary, require the entity or entities subject to an emergency order to provide a detailed account of actions taken to comply with the terms of the emergency order.”<sup>195</sup> Sustained communications links between DOE and BPS entities will be required to meet such requests for information. However, beyond compliance issues, continuous communications will also be required as government and industry partners assess the effectiveness of emergency operations and identify requirements for additional actions.

### Survivability of Communications

Adversaries will have compelling incentives to combine attacks on the grid with strikes against US communications systems. The 2015 attack on Ukraine’s electric grid illustrates the potential benefits of doing so. The perpetrators struck both power distribution systems and the phone networks; the latter attack prevented customers from reporting outages and disrupted grid operators’ ability to conduct restoration operations.<sup>196</sup> In turn, if adversaries can lengthen power outages by disrupting communications systems essential

<sup>193</sup> DOE, “RIN 1901-AB40,” 1181.

<sup>194</sup> DOE, “RIN 1901-AB40,” 1177.

<sup>195</sup> DOE, “RIN 1901-AB40,” 1182.

<sup>196</sup> “Alert (IR-ALERT-H-16-056-01).”



for restoration, those extended blackouts will disrupt electricity-dependent cell towers and other communications-system components as their backup power supplies begin to fail. Simultaneous operations against grid and communications infrastructure will create synergistic, mutually reinforcing disruptions in both sectors.

We should assume that adversaries will design their attacks to maximize multisector failures, especially since they would already be facing the risk of US response operations if they struck the grid alone. We should also assume that as industry and government partners develop increasingly effective plans and capabilities to employ emergency orders, adversaries will seek to disrupt the communications systems essential for industry–government coordination in grid security emergencies. Enemies might strike communications systems to hobble efforts to share preattack threat data and convey emergency orders. Once attacks on the grid were under way, adversaries could also seek to cripple the communications systems needed to coordinate emergency operations and assess requirements for additional measures.

Strengthening the survivability of existing communications links will be essential to manage these risks. To date, ESCC consultation and coordination mechanisms have relied almost entirely on open phone lines and internet-based communications. These systems are vulnerable to distributed denial-of-service attacks and a range of other increasingly severe threats,<sup>197</sup> as well to the loss of the grid-provided electricity on which many such systems depend (especially in long-duration outages that put emergency power assets at risk).

Adversaries may also seek to disrupt systems essential for information sharing. For example, the Cybersecurity Risk Information Sharing Program and other E-ISAC notification procedures and portals are in place to alert utilities when adversaries

are implanting malware on critical systems.<sup>198</sup> This includes the E-ISAC's new Critical Broadcast Program, which is intended to operationalize the organization's information sharing capabilities.<sup>199</sup> The FBI and DHS also issue alerts to the energy sector, as in the case of CrashOverride.<sup>200</sup> However, many of these warning and information sharing mechanisms rely on the internet or other potentially vulnerable systems. Industry and government should explore options to ensure that they can still convey essential data in the face of sophisticated attacks on the communications sector.

In addition, adversaries may seek to disrupt the issuance of emergency orders. DOE's grid security emergency rule notes that the department intends to convey orders through specialized means such as the NERC alert system. This internet-based system is designed to provide concise, actionable information to the electricity industry. Alerts issued under the system can include "essential actions" to protect BPS reliability, which require recipients to respond as defined in the alert.<sup>201</sup> DOE and its industry partners might quickly and easily leverage that process to issue emergency orders to BPS entities.

The NERC alert system also offers advantages in terms of its reach across registered entities. NERC already distributes alerts broadly to BPS users, owners, and operators in North America. Hence, the alert system provides DOE with an opportunity for "one-stop shopping" when issuing emergency orders. The secretary could issue an order to NERC for distribution to both regional operating organizations (regional transmission organizations, independent

<sup>197</sup> Banham, "DDoS Attacks."

<sup>198</sup> "Energy Sector Cybersecurity Preparedness," DOE; and "Electricity Information Sharing and Analysis Center," NERC.

<sup>199</sup> The E-ISAC recently performed a test call for the program, with participation from 1,208 individuals across 245 organizations. See Lawrence, de Seibert, and Daigle, "E-ISAC Update."

<sup>200</sup> "Alert (TA17-163A)."

<sup>201</sup> "About Alerts," NERC.



system operators, reliability coordinators, etc.) and individual BPS power companies.

However, NERC's alert system is email based.<sup>202</sup> As such, it faces many of the same cyber threat vectors and interdependency-related vulnerabilities as the ESCC consultation mechanism. The system also includes only those utilities that are registered as BPS entities and are subject to mandatory, enforceable standards. Utilities that operate purely at the local distribution level are not part of the NERC alert system, even though these utilities may be essential for implementing emergency orders for prioritized load shedding and other actions to sustain power to critical facilities.

Moreover, while the NERC alert system could provide a means of communications across BPS users, owners, and operators, NERC primarily uses the system to communicate alerts of voluntary actions to be taken by electric industry stakeholders. Using the NERC alert system to instead communicate a mandatory action pursuant to a DOE emergency order would require clear coordination and communication to ensure that the order and associated requirements for action are fully understood. In addition, while the NERC alert system offers a proven means to convey unclassified information, the system may not be well suited to distribute classified data.

To fill these gaps, industry and government partners should consider measures to bolster the NERC alert system or create fallback options for survivable communications. Satellite phones offer a prominent option for operational coordination. These phones are widely deployed both among BPS entities and by major distribution-only utilities. A large number of these organizations also regularly exercise for their use when phone and internet-based communications fail.

However, the communications satellites and other infrastructure on which those phones depend could also come under attack in grid security emergencies.

Retired US Air Force General William Shelton, who directed the US Air Force Space Command, has testified that communications satellites are increasingly susceptible to disruption. Potential adversaries "have developed a full quiver of these methods, ranging from satellite signal jamming to outright destruction of satellites via a kill vehicle, such as that successfully tested by China in 2007. The pace of these counterspace efforts appears to be accelerating, and the impact of the use of counterspace capabilities likely would be felt by all sectors of the space community."<sup>203</sup>

Accordingly, power companies are ramping up their investments in terrestrial emergency communications systems that are hardened against cyber and physical attacks and can be used to sustain critical grid functions even if satellite phones fail.<sup>204</sup> Push-to-talk radios, dark fiber systems owned by BPS entities themselves, and other highly survivable systems increase the likelihood that utilities will be able to meet their own core operational needs.

However, only limited efforts are under way to build dark fiber or other survivable links between BPS entities—much less between those entities and DOE. The National Infrastructure Advisory Council study *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* (August 2017) emphasizes the need to establish "separate, secure communications networks specifically designated for the most critical cyber networks, including 'dark fiber' networks for critical control system traffic and reserved spectrum for backup communications during emergencies."<sup>205</sup>

The council's study recommends that DOE and its partners launch a pilot project to create such dedicated communications links. In doing so, DOE should leverage lessons learned from the communications sector and specifically from the National

<sup>202</sup> "About Alerts," NERC.

<sup>203</sup> Shelton, "Threats to Space Assets," 3.

<sup>204</sup> FERC and NERC, *PRASE*, 15.

<sup>205</sup> NIAC, *Securing Cyber Assets*, 7.

Security Telecommunications Advisory Committee, which has extensive experience in building redundant and survivable systems.<sup>206</sup> However, to prepare for grid security emergencies, any such effort should go far beyond the goal of ensuring that utilities “can communicate with utility crews working in the field to manually restore power” and conduct other postattack operations.<sup>207</sup> Survivable communications systems must also be able to coordinate emergency operations across the electricity subsector and with supporting government agencies. Otherwise, emergency orders will offer little value for protecting and restoring grid reliability precisely when those orders are needed most.

### Authenticating and Securing Emergency Orders

In addition to disrupting the availability of communications systems, adversaries may also seek to corrupt the content of emergency orders and coordination messages, and gain access to classified US data to help defeat grid protection measures. One near-term requirement will be to ensure that utilities can authenticate the orders they receive from DOE. Power companies will need to be able to verify that an order has actually come from the secretary, and that adversaries have not altered its content. Verifying the authenticity of orders will be especially important if such orders require extraordinary measures that could further disrupt normal service and affect public health and safety.

Existing mechanisms and protocols to ensure the integrity of subsector communications provide an initial basis to meet these challenges. Other government agencies have also developed authentication protocols that could be adapted for use in grid security emergencies. For example, the *DoD Cybersecurity Discipline Implementation Plan* (February 2016) offers detailed guidance to strengthen authentication in the face of adversary

efforts to exploit communications networks and devices.<sup>208</sup>

Adversaries may also seek to gain access to classified or operationally sensitive emergency orders. When attacks are imminent, it might be desirable to issue orders for targeted malware scrubbing and other operations that would need to be kept covert for as long as possible, lest those operations create incentives for adversaries to strike before their advanced persistent threats were disabled. When attacks are under way, it could be useful to deny adversaries the knowledge of where and how BPS entities are prioritizing the flow of power to vital military bases and other national security facilities. Securing power restoration orders and implementation plans against the enemy will be especially important, given the risk that adversaries will target restoration operations to extend power outages and magnify their political, economic, and military impacts.

The FPA and subsequent grid security emergency rule provide for the sharing of classified information in grid security emergencies. The rule specifies that:

To the extent practicable, and consistent with obligations to protect classified and sensitive information, the Secretary may provide temporary access to classified and sensitive information, at the level necessary in light of the conditions of the incident, related to a grid security emergency for which emergency measures are issued to key personnel of any entity subject to such emergency measures, to the extent the Secretary deems necessary under the circumstances.<sup>209</sup>

That provision is valuable, but additional measures will be necessary to protect classified emergency orders and associated information from adversaries. The E-ISAC and the Cybersecurity Risk Information Sharing Program already have mechanisms and protocols for sharing and securing classified threat

<sup>206</sup> “About NSTAC,” DHS.

<sup>207</sup> NIAC, *Securing Cyber Assets*, 7.

<sup>208</sup> DOD, *DoD Cybersecurity Discipline Implementation Plan*.

<sup>209</sup> DOE, “RIN 1901–AB40,” 1182.

data with BPS entities cleared for access to that data.<sup>210</sup> Industry and government partners should consider building on those mechanisms to support the issuance of classified emergency orders. Ongoing progress under the Cybersecurity Risk Information Sharing Program will be valuable as it serves a growing array of utilities, accesses additional sources of data and advanced analytic tools, and continues other improvements.

DOE and its partners in industry and government might consider sharing this classified data in other ways. For example, DHS and other federal partners such as the FBI and the National Guard have secure video teleconference capabilities. However, these are technologically complex and not seamlessly interoperable with industry systems. Moreover, only a minority of electric companies in the United States have personnel with security clearances necessary to access classified information. Section 215A addresses this issue by ordering the secretary to “facilitate and, to the extent practicable, expedite,” the security clearance process for key personnel of any entity subject to emergency orders to enable “optimum communication” of threat information.<sup>211</sup> DOE should accelerate its ongoing efforts to meet this requirement. The section also grants the secretary and other appropriate federal agencies the authority to provide temporary access to classified information regarding grid security emergencies and subsequent orders to key personnel of complying entities.<sup>212</sup>

Yet, even for utilities with cleared personnel on their staffs, an even smaller number possess the sensitive compartmented information facilities or other infrastructure and government approvals to store classified information. To address those limitations, the grid security emergency rule clarifies that the secretary may declassify information critical to the

emergency response.<sup>213</sup> But declassification and transmission of data over unsecured networks will carry inherent risks of exposure to adversaries. Emergency orders will constitute the domestic equivalent of combatant commander operational plans; when emergency orders may be vulnerable to enemy countermeasures, securing them will be vital to their effectiveness.

### Communicating with the American People

Adversaries may attack the grid not only to disrupt national defense and the economy but also to gain political leverage over US leaders by inciting public panic and disorder. A presidential declaration that the grid faces imminent danger of attack would immediately become a focus of concern and ill-informed speculation in traditional and social media. The onset of such attacks and disruption of electric service would further intensify that focus and create immense challenges for deciding what to tell the US public.

Preplanning for public messaging to accompany grid security emergency declarations will be essential to manage such risks. Grid owners and operators have extensive expertise in communicating with customers in outages caused by hurricanes, wildfires, and other natural hazards. Unifying messaging with governors and other elected officials on estimated restoration times already presents significant challenges in such events. However, those difficulties will be dwarfed by the problems that adversaries can create through cyber attacks. Attackers may:

- Use information warfare campaigns via social media to incite panic concerning the effect of power outages on water systems, hospitals, and other facilities and services vital to public health and safety
- Intensify state and local requests for defense support to civil authorities to deal with these

<sup>210</sup> “Energy Sector Cybersecurity Preparedness,” DOE.

<sup>211</sup> 16 U.S.C. § 824o–1, (e).

<sup>212</sup> 16 U.S.C. § 824o–1, (b)(7).

<sup>213</sup> DOE, “RIN 1901–AB40,” 1778.

anticipated effects, and thereby put pressure on US leaders to divert scarce defense assets and resources from other missions

- Disrupt normal means of communication on which the public will rely for information about the event
- Magnify the inherent difficulties of estimating restoration times by employing advanced persistent threats that enable repeated reattacks and disruptions in grid service until eradicated from BPS networks.

DHS's Social Media Working Group for Emergency Services and Disaster Management has offered preliminary recommendations on how to counter disinformation during disaster response operations.<sup>214</sup> In addition, the ESCC and its members are developing playbooks to help meet disinformation challenges and support public messaging in the event of cyber or physical attacks against the grid.<sup>215</sup> Building on that foundation, DOE, the ESCC, and their partners should collaborate to ensure that presidential grid security emergency declarations are accompanied by communications that address the American people's concerns and strengthen community resilience. Preplanning for message coordination with Canada and Mexico could also be helpful and might leverage the FPA's provisions for such multinational consultations concerning the issuance of emergency orders.<sup>216</sup>

As industry and government partners build communications playbooks to accompany the issuance and implementation of emergency orders, they will need to account for the specific features of those orders and the disruptive impact they may have on normal electric service. For example, some orders that will be valuable for protecting grid reliability, including those for prioritized load shedding, could

cut off electricity to many thousands of customers to preserve service for essential facilities. Emergency orders that could have such effects should be accompanied by preplanned communications playbooks to address customer concerns.

## The Deeper Value Proposition for Emergency Orders: Political Top Cover, Waivers, and Cost Recovery

The grid security emergency provisions of the FPA do not even mention a significant advantage that orders can provide for industry: they can help protect power companies from the political heat that extraordinary grid protection measures will create. The FPA's provisions for regulatory waivers and cost recovery offer more explicit benefits. Yet, given the risks that utilities could incur in conducting emergency operations, and the investments in infrastructure that may be required to facilitate order implementation, Congress and DOE should consider additional measures to help power companies defend the grid and protect national security.

### Facilitating Operations under Extraordinary Political Circumstances

In responding to natural hazards, power companies can fall under intense pressure to serve the priorities of state and local elected officials. In severe weather events, for example, governors have told utilities to delay sending restoration resources to assist neighboring states until service has been restored to *all* customers (i.e., voters) in the governors' own states.

Cyber and physical attacks on the grid could create still more intense political pressure, and complicate utilities' efforts to serve national priorities versus those most urgent to meet state and local needs. Such attacks will occur in the context of broader risks of all-out war and will magnify public fears in ways that hurricanes or other natural hazards cannot—especially if those attacks are accompanied by

<sup>214</sup> Social Media Working Group for Emergency Services and Disaster Management, *Countering False Information*.

<sup>215</sup> ESCC, "ESCC: Electricity Subsector Coordinating Council."

<sup>216</sup> 16 U.S.C. § 824o-1, (b)(3).



information warfare operations to incite public panic. Governors will have powerful incentives to ensure that utilities in their states take care of their own citizens rather than meeting requests for assistance from power companies in other states.

However, from a national security perspective, not all states and customers within them will be of equal importance for protecting defense critical electric infrastructure. Some low-population states served by utilities with only limited resources are the homes of vital military installations. These utilities may need assistance from out-of-state power companies to supplement their own personnel and response capabilities when adversaries strike.

The electric industry's Cyber Mutual Assistance (CMA) Program will be critical for providing such support.<sup>217</sup> DOE is expanding the technical resources and capabilities available to support CMA response operations.<sup>218</sup> Under the national response event initiative, investor-owned utilities (led by the Edison Electric Institute) are also bolstering mechanisms to support restoration efforts for incidents that require assistance from utilities across the United States.<sup>219</sup> All of these initiatives will be vital for responding to grid security emergencies that entail multiregional disruptions of the BPS or degrade critical electric infrastructure that the infrastructure's owners cannot restore on their own.

Yet, the voluntary nature of these mutual assistance systems could present challenges in grid security emergencies. In hurricanes or other natural hazards, governors and utilities can predict whether or not their states are likely to be struck and either husband their resources accordingly or provide them in response to requests for assistance. Cyber and physical attacks by Russia, China, or other potential adversaries are much less predictable. Enemies may

strike one region before moving on to others. Attacks could even occur on a nationwide basis. Accordingly, elected officials may discourage utility leaders from volunteering resources for mutual assistance in neighboring regions, even if their own states have not yet been struck.

Issuing emergency orders can help utilities address these challenges and serve national priorities. Participants in the Cyber Mutual Assistance Program are already taking steps to account for the risk of multiregional attacks. DOE and its industry partners should preplan to reinforce those measures in grid security emergencies. If the secretary orders utilities to help protect or restore grid reliability beyond their service areas, those orders will help justify (and indeed, legally require) providing such assistance, regardless of the political pressure against doing so. DOE should consider reaching out to state and local leaders and their senior energy appointees before emergencies occur in order to ensure that they are familiar with the FPA requirements and the national security value of mutual assistance.

Emergency orders can also help utilities execute politically unpopular emergency operational decisions within their own service areas. Cyber and physical attacks could put utility CEOs in the unenviable position of having to manage shortfalls in available power by depriving lower-priority customers of service to protect the flow of electricity to military bases and other facilities essential to national security. The secretary of energy can give CEOs political top cover for taking such unpopular actions, rather than leave them to act on a voluntary basis and bear the full brunt of explaining why they did so.

Exercises can help utilities and government officials prepare to collaborate in the face of intense political pressures, and coordinate the execution of emergency orders on a nationwide basis. NERC already requires BPS entities to exercise their individual emergency and power system restoration plans. In the GridEx exercise series, over one hundred utilities across the

<sup>217</sup> ESCC, "Cyber Mutual Assistance Program."

<sup>218</sup> DOE, *Multiyear Plan*, 29.

<sup>219</sup> EEI, *Understanding the Electric Power Industry's Response and Restoration Process*.



United States and Canada test the use of their plans against combined cyber-physical attacks and exercise the use of Cyber Mutual Assistance protocols and procedures. Building template emergency orders and utility-specific implementation plans will provide an even stronger basis for coordinated multientity exercises. In planning for GridEx V in 2019, NERC and its government and industry partners should consider the possibility of exercising the issuance and implementation of specific template emergency orders. State, local, tribal, and territorial participation in utility exercises that include the use of emergency orders will also be crucial.

### Environmental, Regulatory, and Legal Waivers

In amending the FPA to address grid security emergencies, Congress provided power companies with an important protection for complying with emergency orders—one that they might not receive by implementing equivalent emergency measures on a voluntary basis. If complying with an emergency order causes a BPS entity to violate FERC-approved grid reliability standards or other rules or provisions under the FPA, the act specifies that those actions “shall not be considered a violation” of those provisions. Such waivers of enforcement apply unless a complying entity acts in a “grossly negligent manner.”<sup>220</sup>

The FAST Act amendments to the FPA also introduced broader protections into section 202(c), absolving entities from violations of federal, state, or local environmental laws or regulations that occur as a result of complying with an order. That provision shields complying entities from “any requirement, civil or criminal liability, or a citizen suit under such environmental law or regulation.”<sup>221</sup> These protections apply to section 215A emergency orders as well.<sup>222</sup>

FPA-based waivers will be especially valuable for certain types of emergency orders. For example, if the secretary issues orders for maximum generation either before or during an attack, companies that operate coal generators on a sustained basis could violate air quality regulations. Emergency orders that create major disruptions in grid service, such as proactively shedding firm load, could also violate NERC’s FERC-approved reliability standards.<sup>223</sup> Separating preplanned power islands from the surrounding grid, and inflicting instabilities on neighboring electric systems in the process, would be certain to violate such standards as well.

The waiver process under the FPA is structured to function automatically. No further adjudication of liability and enforcement issues should be necessary unless DOE determines that a BPS entity has acted with gross negligence. Nevertheless, industry, DOE, and regulators might find it useful to build consensus on the types of waivers that specific template orders should include.

Their discussions could also help address more far-reaching regulatory issues that grid security emergencies may pose. For example, the FPA does not provide waivers for Nuclear Regulatory Commission regulations. However, as BPS entities, nuclear generators may be the subject of emergency orders in a grid security emergency. It is currently unclear if or how the commission would enforce a violation of its regulations by a nuclear generation entity complying with an emergency order. The worst time to adjudicate such a dispute, however, would be in the midst of a grid security emergency. Pre-event discussions will be particularly important given the nuclear fleet’s imperative to protect public health and safety. DOE, the Nuclear Regulatory Commission, and their industry partners will need to ensure that assessments of regulatory issues associated with

<sup>220</sup> 16 U.S.C. § 824o–1, (f)(4).

<sup>221</sup> 16 U.S.C. § 824a, (c)(3).

<sup>222</sup> 16 U.S.C. § 824o–1, (f)(2).

<sup>223</sup> For example, in events such as the September 2011 Arizona–California disturbance, FERC has found that load shedding led to violations of NERC’s reliability standards.

emergency operations take safety considerations into full account.

Preplanning will also be vital for emergency orders that support power restoration by facilitating the replacement of damaged or destroyed transformers. In the FAST Act, Congress found that “the storage of strategically located spare large power transformers” and other critical grid components “will reduce the vulnerability of the United States to multiple risks facing electric grid reliability,” including cyber and physical attacks.<sup>224</sup> Accordingly, Congress required DOE to develop a strategic transformer reserve plan to determine the number and type of spare large power transformers that should be stored and to examine issues associated with transporting those spares.<sup>225</sup>

DOE responded to this requirement by providing a strategic transformer reserve report (March 2017). The report concludes that industry-led spare transformer programs, including the Spare Transformer Equipment Program and Grid Assurance program, provide a more substantial pool of spare large power transformers than DOE had anticipated and that a federally owned reserve is not needed.<sup>226</sup> However, the plan also found that it was crucial to ensure that large power transformers can be efficiently moved during national emergencies.<sup>227</sup>

Regulatory waivers can play a critical role in facilitating that movement. The higher-voltage classes of large power transformers, including 765-kilovolt transformers, are as big as a house and can be moved—slowly and very carefully—only by specialized heavy-haul trucks, railcars, and barges. Under the auspices of the ESCC, utilities have established the Transformer Transportation Working Group to analyze the problems posed by moving large power transformers in an emergency

and to build collaborative plans with transportation companies and associations. A central finding of the group’s analysis: regulatory waivers will be critical to expedite the movement of large power transformers, especially over roads (including major highways) where normal traffic will need to be limited or temporarily halted.<sup>228</sup>

DOE’s 2017 transformer report committed the department to coordinating with the Transformer Transportation Working Group “to improve and optimize transportation planning in response to a significant national event impacting the electricity grid.”<sup>229</sup> However, the report did not examine how emergency orders and implementation plans might speed the transportation of large power transformers. As DOE collaborates with the working group and with the programs that can provide spare transformers in grid security emergencies, those efforts should identify the existing regulations, permitting requirements, and inspection protocols that are not addressed by the FPA and that pose the greatest impediments to transformer movement. DOE and its partners should then preplan to waive these provisions if the secretary issues emergency orders.

The challenge for such preplanning: the secretary of energy lacks the statutory authority to waive key transportation regulations. Most federal transportation regulations, including those under the purview of the Federal Highway Administration and the Federal Railroad Administration, fall under the authority of DOT. Federal regulations and emergency operations that would govern the movement of transformers on barges, which could be critical for restoring power for coastal cities and along the Mississippi–Ohio river system of inland waterways, are overseen by the US Coast Guard and the US Army Corps of Engineers. State and local transportation regulations and permitting requirements will also

---

<sup>224</sup> FAST Act, 1779.

<sup>225</sup> FAST Act, 1780–1782.

<sup>226</sup> DOE, *Strategic Transformer Reserve*, 21.

<sup>227</sup> DOE, *Strategic Transformer Reserve*, 1.

---

<sup>228</sup> ICF, *Assessment of Large Power Transformer Risk Mitigation Strategies*, 22–23.

<sup>229</sup> DOE, *Strategic Transformer Reserve*, 22.

pose major impediments to moving large power transformers over roads unless adequate waivers are in place to lift restrictions.

DOE should build collaborative plans to employ waiver authorities beyond those directly under the secretary's control. For example, to facilitate the movement of large power transformers, gubernatorial disaster declarations could help waive state-level regulations. The American Association of State Highway and Transportation Officials and National Emergency Management Association are exploring the use of these and other waiver authorities. DOE is also preplanning with other federal, state, local, tribal, and territorial agencies to coordinate response operations under Emergency Support Function #12—Energy.<sup>230</sup> Especially valuable, a growing number of individual power companies are creating contingency plans for emergency transportation with government agencies and road, rail, and barge companies. Building on these efforts, and on initiatives led by the Transformer Transportation Working Group,<sup>231</sup> the electricity subsector and its partners should establish systematic, nationwide plans to facilitate the movement of transformers and other critical equipment in grid security emergencies.

Over the longer term, Congress, industry, and government partners should also consider whether complying entities should have liability protections beyond those currently provided by the FPA. Prioritized load shedding for extended periods will create “winners and losers” in the allocation of power and could put lives at risk. In severe grid security emergencies, sustaining the flow of power to regional hospitals and other section 9+ assets may leave shortfalls in electric service at dialysis centers, small urgent-care centers, and facilities for special-needs citizens. These disruptions will put lives at risk. Legislators, DOE, and electric industry leaders should examine whether utilities complying

with such necessary but highly disruptive emergency orders ought to have additional liability protections. Cutting off power to lower-priority industrial or commercial customers could also expose utilities to lawsuits aimed at recovering lost business revenue or requiring other forms of economic compensation.<sup>232</sup> Again, if these risks of exposure are sufficiently severe, Congress should consider providing further protections for BPS entities.

### **Cost Recovery for Emergency Operations and Support for Investments in Grid Infrastructure**

Complying with emergency orders may force utilities to incur costs beyond their normal operating expenses. The FPA states that if FERC determines “that owners, operators, or users of critical electric infrastructure have incurred substantial costs” in complying with an emergency order, FERC shall “establish a mechanism that permits such owners, operators, or users to recover such costs.”<sup>233</sup> Emergency orders that require generator owners to operate at maximum generation exemplify the additional costs that compliance could create; many other orders could require reimbursement through FERC-directed mechanisms as well.

The act takes a different approach regarding costs incurred in protecting the reliability of defense critical electric infrastructure. The FPA states that to the extent that emergency orders require utilities responsible for defense critical electric infrastructure to take emergency measures, the “owners or operators” of critical defense facilities that rely on such infrastructure “shall bear the full incremental costs of the measures.”<sup>234</sup> Fair warning to DOD: it

<sup>230</sup> “State and Local Energy Assurance Planning.” DOE.

<sup>231</sup> DOE, *Strategic Transformer Reserve*, 12.

<sup>232</sup> Frankel, “Can Customers Sue Power Companies for Outages?”

<sup>233</sup> The FPA also specifies that to be eligible for cost recovery, complying entities must also have incurred their costs “prudently” and that those costs “cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users.” 16 U.S.C. § 824o–1, (b)(6)(A).

<sup>234</sup> 16 U.S.C. § 824o–1, (b)(6)(B).

should be prepared to reimburse power companies for the additional spending needed to protect or restore service to military bases in grid security emergencies.

FERC and DOD could establish these reimbursement mechanisms after attacks have been defeated and utilities have restored the grid to normal service. By that point, however, generation asset owners, transmission operators, and other BPS entities may already be defaulting on their debts and teetering on the brink of financial collapse, especially if:

- attacks create major blackouts and deprive utilities of revenue;
- emergency operations require significant additional spending on response personnel, equipment replacement, and other expenses; and
- adversaries disrupt financial markets, either through direct cyber attacks or as a result of the loss of electricity and other critical services, and utilities are unable to access emergency loans and other forms of liquidity.<sup>235</sup>

Power companies are strengthening their plans and capabilities for cross-sector support with the financial services sector.<sup>236</sup> These efforts should include the development of contingency plans for financial-services companies (in coordination with the Department of Treasury and DOE) to help utilities cover the urgent expenses they may incur in responding to grid security emergencies. In addition, to facilitate the reimbursement process provided for in the FPA, FERC should partner with DOE and power companies to develop mechanisms and criteria long before adversaries strike the grid. As with the creation of emergency orders themselves, establishing guidelines and processes to cover the costs of complying with orders will be more difficult once attacks are under way.

Cost recovery for investments in grid infrastructure to facilitate emergency order implementation will pose an additional challenge. Many promising emergency orders, including those for conservative operations, can help protect or restore grid reliability without requiring new spending on transmission lines or other assets. Other orders may be impossible to execute unless BPS entities make additional investments in infrastructure. It will be near useless to order transmission operators to protect or rapidly restore service to vital but remote military bases served by a single transmission line if adversaries destroy the single line on which they depend. Constructing independent redundant transmission lines and supporting infrastructure to serve such facilities may therefore be a prerequisite to ensure that these facilities can help defeat US adversaries when the nation is under attack. DOD will need to develop a cost-recovery mechanism to reimburse defense critical electric infrastructure owners for making such investments.

To be even remotely viable as an emergency order design option, most preplanned power islands will also require at least some infrastructure construction. Ideally, these preplanned islands will use existing generation, transmission, and distribution assets within their service footprints to separate from the grid and still be able to provide reliable electric service to the section 9+ assets inside their borders. But many areas that might be designed to function as islands in a grid security emergency will lack adequate infrastructure to do so. The grid's interconnected design enhances the reliability of electric service by ensuring that redundant pathways exist to serve loads when interruptions occur. Preplanned power islands will not only lose those reliability benefits, but they will also have to make do with infrastructure that utilities built and aligned to be supporting components of the interconnected grid—not self-sustaining islands that would be stood up in grid security emergencies. Moreover, operating and recovering from preplanned island schemes will create an entirely different operating mode than industry is currently designed

<sup>235</sup> NERC, *GridEx III Report*, 15.

<sup>236</sup> See, for example, the Strategic Infrastructure Coordinating Council (SICC). ESCC, "ESCC: Electricity Subsector Coordinating Council."



for. Further studies will need to examine the potential investment requirements that such islands could entail, along with the myriad other challenges that their design and operation would pose. But the larger point remains: to be effectively implemented, many emergency orders could require spending on new transmission lines and other grid infrastructure.

The FPA provisions for grid security emergencies do not explicitly authorize reimbursement for infrastructure investments. While the act requires FERC to establish a mechanism to enable owners, users, and operators of critical and defense critical electric infrastructure to recover their costs of complying with emergency orders, those funding provisions do not mention preattack investments necessary to facilitate compliance. Fortunately, FERC already has clear criteria and mechanisms for employing tariffs, rate adjustments, and other means to enable BPS entities to recover costs for infrastructure investments in resilience against cyber and physical attacks.<sup>237</sup> FERC, DOE, and their industry partners should discuss how those existing mechanisms might be applied to help fund prudent, high-impact investments to facilitate emergency order execution.

Similar discussions will be necessary with state public utility commissions. As noted above, local distribution systems will play vital roles in implementing emergency orders. Public utility commissions have primary regulatory authority over such distribution systems and are typically responsible for determining whether proposed infrastructure investments are prudent and eligible for cost recovery. They could also make important contributions to reviewing proposed implementation plans for emergency orders that would be executed within their respective states, particularly when local distribution systems would be necessary to implement the orders.

<sup>237</sup> See, for example, FERC, *Extraordinary Expenditures* (96 FERC ¶ 61,299), 1; FERC, *Policy Statement on Matters Related to Bulk Power System Reliability* (107 FERC ¶ 61,052), 10–11; and FERC, *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events* (156 FERC ¶ 61,215), 60.

The FPA opens the door to such discussions. The act states that FERC and the secretary of energy “shall take into consideration the role of State commissioners in reviewing the prudence and cost of investments, determining the rates and terms of conditions for electric services, and ensuring the safety and reliability of the bulk-power system and distribution facilities within their respective jurisdictions.”<sup>238</sup> Initiating these discussions with the National Association of Regulatory Utility Commissioners (NARUC) would offer an especially efficient way forward. Over the past decade, NARUC has extensively analyzed criteria for assessing the prudence of investments against cyber and physical attacks and has developed close working relationships with FERC to coordinate across their respective regulatory realms. NARUC, FERC, and the electric industry should apply those collaborative relationships to address the challenges of cost recovery and integrated implementation planning that emergency orders entail.

## Conclusions and Recommendations for Broader Progress

Taken together, the options for industry–government collaboration examined in this report constitute a massive undertaking for which Congress appropriated zero funding to utilities. Developing a sequenced, prioritized strategy to explore these options will help make doing so a more manageable task.

Potential emergency orders will differ not only in terms of the phases of an attack in which they would be most useful, and in the degree to which they will disrupt normal electric service, but also in how difficult they will be to develop. Orders for many conservative operations will be relatively easy to create—especially those that fall into the no-regrets category. Utilities frequently use conservative operations to help protect grid reliability in severe weather events. A growing number of companies are

<sup>238</sup> 16 U.S.C. § 824o–1, (d)(4).



already building on that foundation to draft equivalent conservative operations against cyber and physical threats. Emergency orders based on these initiatives constitute “low-hanging fruit”; creating such orders offers an immediate opportunity for industry and government to bolster grid resilience and also build co-development mechanisms that could be applied to more challenging emergency order initiatives.

However, it would be a mistake to delay analysis of more difficult and problematic orders. Prioritized load shedding and other extraordinary measures may be essential to help grid owners and operators protect BPS reliability when attacks are under way, especially if adversaries are on the brink of creating cascading failures. Long-lead analysis should begin immediately on potential orders that present immense design challenges but could also offer unique benefits for national security. Improving communications survivability and preplanning to counter disinformation campaigns will also be crucial for grid security emergency preparedness. So, too, will be efforts not only to fully leverage the FPA’s regulatory waiver and cost recovery mechanisms but also to explore additional liability protections and other measures to help entities comply with emergency orders.

A comprehensive plan to align and integrate these initiatives should also address three additional opportunities to build resilience for grid security emergencies: (1) preplanning to use additional federal and state emergency authorities to defend natural gas systems, communications networks, and other infrastructure on which the grid depends; (2) coordinating with Canada, Mexico, and other nations whose grids may be struck in conjunction with attacks on US electric systems; and (3) exploring new options to deter and defeat attacks on the grid by integrating defensive measures with government operations to blunt further strikes on US power companies and other targets.

## Employing Additional Emergency Authorities for Cross-Sector Resilience

Building preparedness against attacks on the grid is necessary but not sufficient to protect BPS reliability. In many US regions, power generation is becoming extraordinarily dependent on the flow of natural gas. Adversaries may attempt to cause cascading blackouts and other major grid instabilities by crippling natural gas systems. To hedge against such disruptions, some generators have the ability to operate on diesel and other secondary fuels if attackers interrupt gas supplies. But the refining and transportation systems needed to resupply such “dual-fuel” generators with diesel will themselves be at risk in grid security emergencies.<sup>239</sup> Moreover, as examined earlier in this report, coordinated grid restoration will also depend on the availability of communications systems and other infrastructure sectors.

This report has focused on employing the emergency authorities that Congress incorporated into the FPA by creating section 215A of the act in 2015. However, these authorities apply only to BPS owners and operators. The secretary cannot issue emergency orders under 215A to operators of natural gas and diesel fuel systems, much less to telecommunications companies and other infrastructure owners beyond the energy sector. The secretary has a range of other emergency authorities, including the Defense Production Act (DPA) and the authorities provided by section 202(c) of the FPA, which could facilitate coordinated response and restoration operations across the energy sector. The analysis that follows examines how DOE and its industry partners could preplan for the integrated use of all such authorities in a grid security emergency. This analysis also examines how federal and state leaders might use additional emergency powers to coordinate multisector response operations.

---

<sup>239</sup> The author has advised Exelon Corporation on risks of fuel interruptions for power generation. Exelon has provided no funding for this report.

## Coordinating Emergency Operations among Electric Utilities, Natural Gas Systems, and Other Energy Sector Components

Natural gas is an increasingly important source of fuel for power generation in many regions of the United States. Between 2002 and 2016, the nationwide share of electricity provided by gas-fired units increased from 18 percent to approximately 34 percent.<sup>240</sup> However, in New England, California, and other parts of the United States, natural gas has become the predominant source of fuel for power generation.

ISO New England has highlighted the risks that this reliance creates for grid resilience. It notes that “in New England, the most significant resilience challenge is fuel security—or the assurance that power plants will have or be able to obtain the fuel they need to run, particularly in winter—especially against the backdrop of coal, oil, and nuclear unit retirements, constrained fuel infrastructure, and the difficulty in permitting and operating dual-fuel generating capability.”<sup>241</sup>

Other regions also face growing fuel supply risks to grid resilience. A DOE-sponsored report titled *Reliability, Resilience and the Oncoming Wave of Retiring Baseload Units, Volume I: The Critical Role of Thermal Units During Extreme Weather Events* (March 2018) notes that many regional transmission organizations and independent system operators will face a combined challenge of inadequate natural gas pipeline infrastructure and competing demands for fuel from users apart from power generators.<sup>242</sup> More broadly, NERC has found that “the electric sector’s growing reliance on natural gas raises concerns regarding the ability to maintain BPS reliability when facing constraints on the natural

gas delivery systems.”<sup>243</sup> NERC’s 2016 *Long-Term Reliability Assessment* also notes that “as part of future transmission and resource planning studies, planning entities will need to more fully understand how impacts to the natural gas transportation system can impact electric reliability.”<sup>244</sup> Additionally, in *Grid Resilience in RTOs and ISOs* (January 2018), FERC called for additional data to better assess the risks posed by “wide-scale disruption to fuel supply” that could result in outages of multiple generators.<sup>245</sup>

Companies in the oil and natural gas subsector are bolstering their capabilities to protect their critical system components from attack and are taking new measures to ensure the continued safe and reliable delivery of natural gas to critical customers, including power generators.<sup>246</sup> However, threats to the oil and natural gas subsector are rapidly escalating as well.<sup>247</sup> As gas system owners and operators address these increasing threats, new opportunities will emerge for joint gas–electric resilience initiatives and emergency planning.

The oil and natural gas and electricity subsectors are already improving their coordination on resilience issues.<sup>248</sup> Moreover, NERC has been facilitating coordination between BPS entities and natural gas companies to address fuel resilience and interdependency challenges.<sup>249</sup> The ESCC has also been developing new coordination mechanisms for the

<sup>240</sup> DOE, *Staff Report to Secretary*, 90.

<sup>241</sup> ISO-NE, “Response of ISO New England Inc.,” 1.

<sup>242</sup> NETL, *Reliability, Resilience and the Oncoming Wave*, 4, 14, 22, 3.

<sup>243</sup> NERC, *Short-Term Special Assessment*, 12. See also NERC, *2013 Special Reliability Assessment*.

<sup>244</sup> NERC, *2016 Long-Term Reliability Assessment*, 21.

<sup>245</sup> FERC, *Grid Resilience*, 161 FERC ¶ 61,012 (2018), 14. See also Stockton, *Prepared Direct Testimony on Grid Reliability and Resilience Pricing*.

<sup>246</sup> “Cybersecurity,” American Gas Association.

<sup>247</sup> Sobczak, Northey, and Behr, “Cyber Raises Threat”; and Stockton (on behalf of Exelon Corporation), *Prepared Direct Testimony* (Docket No. RM18-1-000), 13.

<sup>248</sup> DOE, *Staff Report to Secretary*, 94; and EIS Council, *E-PRO Handbook II*, 189.

<sup>249</sup> NERC, *Reliability Guideline: Gas and Electrical Operational Coordination Considerations*, 1.

two industries (as well as with communications and financial services sectors).<sup>250</sup> Additionally, the natural gas industry participated in GridEx IV, which examined opportunities to mitigate the risk that adversaries will simultaneously attack gas and electric systems.

Building on these and other collaborative efforts, gas and electric companies (and their regulatory partners) should examine how they can prioritize support for each other in grid security emergencies. For example, when blackouts occur, electric companies typically prioritize the restoration of service to compression stations and other electricity-dependent gas infrastructure that is essential to supply fuel for power generation and other critical customers. Support for gas infrastructure should remain a priority, even as BPS entities add other section 9+ facilities to their restoration plans. Gas companies might also reassess their curtailment policies to help gas-dependent BPS entities sustain service to major military installations and other vital facilities in grid security emergencies.<sup>251</sup>

BPS entities and DOE should also pursue deeper collaboration with the companies that refine and deliver secondary fuels for power generation. If adversaries interrupt the flow of natural gas, dual-fuel generators can use diesel, no. 2 fuel oil, or other secondary fuels to sustain their operations in a grid security emergency.<sup>252</sup> However, cascading blackouts could disrupt the flow of these secondary fuels as well. Refining and transportation systems components that are essential to resupply dual-fuel generators depend on electricity. Adversaries may also attack these systems at the same time they strike the grid. Moreover, ongoing cutbacks in industry delivery capacity could magnify these risks of interruption. ISO New England notes that a “withering

delivery supply chain” constitutes an “unquantifiable X factor” in assessing grid resilience.<sup>253</sup> Preplanning to prioritize the delivery of secondary fuels for power generation will be essential for grid security emergencies, especially given the enormous demand for diesel from emergency power generators from hospitals, water utilities, and other vital facilities in wide-area blackouts.

Emergency authorities beyond 215A can help prioritize the flow of natural gas and secondary fuels to protect and restore grid reliability. The DPA will be especially helpful in this regard. The act is the “primary source of presidential authority to expedite and expand the supply of critical resources from the U.S. industrial base to support the national defense and homeland security.”<sup>254</sup> The DPA defines national defense to include “critical infrastructure protection and restoration,” encompassing all electric system components and supporting fuel supply infrastructure (including natural gas pipelines) that are at risk of cyber and physical attacks.<sup>255</sup> In 2012, the White House delegated many of the president’s DPA authorities to the heads of relevant federal agencies, including the secretary of energy for prioritization and allocation decisions regarding “all forms of energy.”<sup>256</sup>

Especially valuable for cross-sector resilience, DOE has established an Energy Priorities and Allocations System that enables the department to prioritize contracts for the delivery of natural gas, diesel, and other energy resources between the companies that provide them and government agencies, electric utilities, and other private and public sector customers. The system also enables DOE to allocate energy materials, services, and facilities to promote

<sup>250</sup> ESCC, “ESCC: Electricity Subsector Coordinating Council.”

<sup>251</sup> EIS Council, *E-PRO Handbook II*, 219.

<sup>252</sup> ISO-NE, *Operational Fuel-Security Analysis*, 52; and NERC, *2013 Special Reliability Assessment*, 4.

<sup>253</sup> ISO-NE, *Operational Fuel-Security Analysis*, 14, 16.

<sup>254</sup> DHS, *Power Outage Incident Annex*, 129.

<sup>255</sup> 50 U.S.C. § 4552, (14).

<sup>256</sup> Obama, *Executive Order—National Defense Resources Preparedness*.

“critical infrastructure protection and restoration” and emergency preparedness.<sup>257</sup>

DOE has already used its authorities under the DPA to support power generation in previous energy crises. In 2001, for example, the department used these authorities to ensure that emergency supplies of natural gas continued to flow to Californian power generators, thereby helping to avoid threatened electrical blackouts.<sup>258</sup> Now, to build preparedness for grid security emergencies, DOE and its industry partners should consider preplanning to use the DPA to sustain or restore gas and diesel deliveries to critical generators, including those that serve microgrids on defense installations, regional hospitals, and other assets critical for national security and public health and safety.

DOE could use the DPA to support and prioritize power restoration operations in other ways as well. Section 101(a) of the act provides DOE with the authority to prioritize the delivery of critical grid components in an emergency. If coordinated physical attacks damage or destroy transformers at a large number of critical substations, the secretary could use the DPA to allocate replacement transformers in ways that most directly benefit national security and public health and safety.

Two additional sources of emergency authorities could further strengthen preparedness and supplement the use of section 215A emergency orders. The first is section 202(c) of the FPA. The section authorizes the secretary to order “temporary connections of facilities and such generation, delivery, interchange, or transmission of electric energy as in its judgment will best meet the emergency and serve the public interest.” That provision also specifies that the secretary could exercise such powers “during the continuance of any war in which the United States is engaged, or whenever the Commission determines that an

emergency exists by reason of a sudden increase in the demand for electric energy, or a shortage of electric energy or of facilities for the generation or transmission of electric energy, or of fuel or water for generating facilities, or other causes.”<sup>259</sup>

A key virtue of section 202(c) is that the secretary can apply these emergency authorities to local distribution systems that might not fall within the purview of section 215A. Moreover, DOE has a strong record of having used 202(c) authorities in past emergencies, including the California Enron crisis, Hurricane Katrina, and other events.<sup>260</sup> DOE and its industry partners should consider building on this foundation to plan for the use of these authorities in grid security emergencies.

The Natural Gas Policy Act provides further authorities that could help coordinate energy sector operations in grid security emergencies. The president must declare a natural gas supply emergency before the secretary gains emergency powers under the act. The president can make such a declaration if there is evidence of an imminent or existing “severe natural gas shortage, endangering the supply of natural gas for high-priority uses” and that, having exhausted other alternatives “to the maximum extent practicable,” natural gas emergency authorities are necessary to resolve the situation.<sup>261</sup> The president may also delegate this authority, as well as the authority to issue rules or orders, to the secretary of energy or other appropriate federal officials.<sup>262</sup>

The president or secretary can issue two main types of orders or rules. Most important, during a natural gas supply emergency, the act authorizes the president or other officials to allocate natural gas supplies “to assist in meeting natural gas requirements for high-priority

<sup>257</sup> DOE, “RIN 1901-AB28,” 33615, 33622-33626.

<sup>258</sup> Brown and Else, *Defense Production Act of 1950*, 10.

<sup>259</sup> 16 U.S.C. § 824a, (c)(1).

<sup>260</sup> “DOE’s Use of Federal Power Act Emergency Authority,” DOE.

<sup>261</sup> 15 U.S.C. § 3361, (a).

<sup>262</sup> 15 U.S.C. § 3364, (d).



uses.”<sup>263</sup> The secretary could use this provision to ensure that critical generating facilities get the fuel they need.

Of course, some of these authorities overlap. DOE and its government and industry partners should develop an integrated approach to employing these powers for grid security emergencies, and determine which particular authorities are best suited to meet specific energy sector risks that cyber and physical attacks can create. These partners, along with other energy sector stakeholders, should also consider exercise scenarios that involve the simultaneous use of multiple emergency authorities to simulate the complex legal environment they may be faced with in a grid security emergency.

### **Multisector Resilience for Grid Security Emergencies**

An overarching strategy for grid security emergency preparedness should also advance operational coordination between energy companies and other infrastructure sectors that both rely on electricity and play vital roles in power restoration. Additional federal emergency authorities and incident response plans can help strengthen coordination between these interdependent sectors.

Using this broader array of plans and authorities will be particularly important if adversaries simultaneously attack multiple infrastructure sectors. By striking other sectors together with the grid, adversaries can exploit interdependencies between them to maximize the attack’s disruptive effects on national security, including the ability of defense installations and supporting civilian infrastructure to conduct operations abroad.<sup>264</sup> The *National Cyber Incident Response Plan* provides a framework for strengthening multisector coordination mechanisms for such attacks. As the administration refines the

plan, DOE and its government and industry partners should ensure that the issuance and execution of emergency orders fit within this broader framework and directly contribute to multisector resilience.

Updates to the *National Response Framework* and other FEMA-led initiatives can offer further benefits for grid security emergencies. In its after-action report from the 2017 hurricane season, FEMA noted that emergency managers and their private sector partners lack the multisector coordination mechanisms necessary to accelerate the restoration of electric power and other lifeline services.<sup>265</sup> The report called for FEMA to build “a cross-sector approach to the Agency’s planning, organizing, response, and recovery operations,” and revise current national-level planning frameworks to create a cross-sector emergency support function.<sup>266</sup> DOE and industry should partner to prioritize support for power sustainment and restoration within this broader initiative.

The *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans* provides a prime opportunity to embed cross-sector coordination efforts in regional incident response plans.<sup>267</sup> The annex calls for the development of regional plans to build resilience against extended multistate blackouts and ensure that interdependent sectors can accelerate power restoration while also countering threats to public health and safety.<sup>268</sup> In many areas of the United States, utilities are already helping DOE, FEMA, and their state and local partners build such plans for their regions. Cross-sector preparedness for grid security emergencies should become a key focus of future power outage incident planning efforts.

---

<sup>263</sup> 15 U.S.C. § 3363, (a).

<sup>264</sup> Homeland Security Advisory Council, *Final Report of the Cybersecurity Subcommittee*, 11.

---

<sup>265</sup> FEMA, *2017 Hurricane Season FEMA After-Action Report*, 13.

<sup>266</sup> FEMA, *2017 Hurricane Season FEMA After-Action Report*, 12–13.

<sup>267</sup> EIS Council, *E-PRO Handbook III*, 45.

<sup>268</sup> DHS, *Power Outage Incident Annex*, 77.



In all of these planning and operational coordination initiatives, DOE and other departments responsible for specific infrastructure sectors should examine how other federal emergency authorities might supplement those that apply to the energy sector. The communications sector provides one such opportunity. The president has extensive authorities to address national security and emergency preparedness telecommunications issues under the Communications Act, including the power to prioritize the use of communications capabilities and provide complying entities with legal and regulatory protections.<sup>269</sup> Executive Order 13618 assigns many of these authorities and associated responsibilities to federal departments and agencies. The secretary of commerce, for example, is responsible for developing plans and procedures for emergency use of radio frequencies and other communications systems.<sup>270</sup> The secretary of homeland security is responsible for overseeing the development, testing, and implementation of emergency communications capabilities.<sup>271</sup> Using these capabilities to support power restoration could be enormously helpful in grid security emergencies. Equivalent emergency authorities for other sectors could assist restoration as well. However, as with all such opportunities, effectively using these federal authorities will depend on extensive preplanning.

State governors are likely to invoke their own authorities to respond to grid security emergencies. Governors have primary responsibility for protecting the health and safety of their citizens. Cyber and physical attacks on the grid, especially if paired with strikes against communications systems and other interdependent sectors, could disrupt hospitals, water systems, and other assets on which their citizens rely. Governors in every state have the ability to declare emergencies and issue executive orders to help deal

with such threats to public health.<sup>272</sup> A growing number of states are also including utility representatives in their emergency operations centers, building collaborative plans and coordination mechanisms to respond to attacks on the grid, and preparing for state National Guard personnel to help utilities defend and restore the flow of power. These initiatives are bolstering overall preparedness for grid security emergencies. However, if multiple governors employ their own emergency authorities and implement state-level blackout response plans, it will be enormously difficult to coordinate their efforts with federal actions—including the issuance of DOE emergency orders to utilities in those very same states.

The only way to overcome such difficulties is to exercise the use of all of the authorities that could help protect and restore grid reliability, across multiple sectors and with the participation of both federal and state leaders. GridEx IV offered an important step forward in this regard. Exercise participants from the oil and natural gas subsector, as well as the financial-services and communications sectors, contributed perspectives on how they could help utilities respond to cyber and physical attacks on the grid. Representatives from state governments discussed how governors might act in such an emergency. GridEx V will provide an opportunity to address such coordination challenges in greater detail. GridEx V could also exercise the use of specific template emergency orders, together with communications mechanisms and playbooks developed for grid security emergencies. Additional exercises by BPS entities and their partners at all levels of government will also be vital to prepare for the implementation of such orders.

## Extended Partnership Requirements within the United States and Abroad

Congress implicitly imposed geographic constraints on the secretary's authority to issue emergency orders to protect the reliability of defense critical electric

<sup>269</sup> 47 U.S.C. § 606.

<sup>270</sup> Obama, *Executive Order—Assignment*, section 5.3.

<sup>271</sup> Obama, *Executive Order—Assignment*, section 5.2. See also DHS, "Emergency Communications."

<sup>272</sup> Orenstein and White, "Emergency Declaration Authorities."

infrastructure. The FPA limits such infrastructure to that which is located in the forty-eight contiguous states or the District of Columbia.<sup>273</sup> However, Alaska and Hawaii are home to vital grid-dependent military installations and supporting civilian infrastructure, including facilities for US continental ballistic missile defense and command and control of military operations in the Pacific region. Key defense installations also exist in Guam and other US territories. As the electric industry and DOE build preparedness for grid security emergencies, they should consider collaborating with the utilities that serve these states and territories and their government partners (including DOD) to strengthen plans and capabilities for coordinated operations.

Close coordination will also be necessary with Canada. The secretary of energy has no authority to issue emergency orders to power companies in other countries. However, the electric grids of the United States and Canada are deeply interconnected. This integration entails both risks and opportunities in grid security emergencies. Adversary-induced blackouts in one nation may cascade across the border, and extraordinary measures taken to restore US grid reliability could affect Canadian systems. Yet, the connectivity between US and Canadian electric systems can also provide unique opportunities to strengthen the security and emergency preparedness of both nations.

A key foundation for binational cooperation in grid security emergencies is already in place. NERC's reliability standards apply to both US and Canadian utilities, providing shared planning and emergency coordination mechanisms on both sides of the border. US and Canadian power companies and government officials should explore how they might supplement these existing mechanisms for

grid security emergencies. The most immediate opportunity to do so will lie in government-to-government consultations. The FPA requires that, to the extent practicable, the secretary of energy shall consult with Canadian authorities before issuing emergency orders.<sup>274</sup> However, the FPA provides no details on the mechanisms by which consultations will be conducted or on whether and how Canadian officials should be informed when the secretary issues emergency orders to US utilities. The analysis that follows examines opportunities to facilitate binational consultation and operational coordination in grid security emergencies.

The FPA also requires that the secretary consult with the Mexican government before issuing emergency orders. While the US and Mexican grids are much less integrated than those of the US and Canada, discussions on grid security emergency preparedness with Mexican officials could also be valuable. Coordination beyond North America may be useful as well. If a severe regional crisis escalates into attacks on the US power grid, US security partners in those regions may face strikes against their own electric systems. Sharing information on whether an attack is imminent and taking coordinated grid protection measures (including those for conservative operations) will help the United States and its allies meet such challenges.

### **Deepening Integration between US and Canadian Grids: Risks and Potential Benefits for Grid Security Emergency Resilience**

DOE notes that "the United States and Canada serve as a global model of highly functional, cross-border electricity coordination."<sup>275</sup> US and Canadian grids are connected by over three dozen major transmission lines, ranging from the Pacific Northwest to New England. The resulting power flows have created a deeply integrated network of north-south BPS infrastructure and synchronized

<sup>273</sup> 16 U.S.C. § 824o-1, (a)(4). The FPA's section on electric reliability, including the definition of BPS, also excludes entities in Alaska and Hawaii, further constraining the authority of the secretary to issue emergency orders to such entities. See 16 U.S.C. § 824o, (k).

<sup>274</sup> 16 U.S.C. § 824o-1, (b)(3).

<sup>275</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6-5.

cross-border operations.<sup>276</sup> This integration also provides significant economic and energy security benefits for both countries.<sup>277</sup>

Connectivity between US and Canadian grids will grow still closer in the decades to come.<sup>278</sup> New York and Massachusetts are pursuing significant increases in Canadian hydropower to help achieve their clean energy goals. Several new cross-border transmission lines are also under development, though many of them face permitting challenges. The Lake Erie Connector is a one-thousand-megawatt high-voltage, direct current line expected to link Ontario's Independent Electricity System Operator with PJM in 2020.<sup>279</sup> The Champlain Hudson Power Express from Quebec to New York City is expected to go into service in 2021, with still other projects in various phases of development in New England, the Midwest, and the Pacific Northwest.<sup>280</sup>

These and other projects offer significant economic benefits to both nations. However, the connectivity of US and Canadian power grids also creates risks of cross-border failures. The 2003 Northeast blackout that started in Ohio created power outages for millions of customers in Ontario.<sup>281</sup> Interconnections between US and Canadian power systems have increased since that event. US and Canadian officials warn that given this connectivity, "isolated or complex events with cascading effects that take place in either country can have major consequences for both the United States' and Canada's electric grids and adversely affect national security, economic stability, and public health and safety."<sup>282</sup>

Mandatory reliability standards reduce the risks of outages across North America. In the aftermath of the 2003 blackout, NERC began issuing standards applicable to entities on both sides of the border. NERC reliability standards are mandatory and enforceable in the provinces of Ontario, New Brunswick, Alberta, British Columbia, Manitoba, and Nova Scotia. Twelve such reliability standards also went into effect in Quebec in April 2015; the province is now considering adopting additional standards.<sup>283</sup> These shared US-Canada standards help power companies in both countries maintain the reliability of their systems and will help them prevent instabilities from spreading during grid security emergencies.

NERC's role as the electric reliability organization for North America provides an additional bulwark for binational grid resilience. As Figure 7 illustrates, three NERC regional entities include power companies on both sides of the border: the Northeast Power Coordinating Council (NPCC), the Midwest Reliability Organization (MRO), and the Western Electricity Coordinating Council (WECC). These entities help monitor and enforce compliance with reliability standards and reinforce NERC's integrated approach to reducing the risks of cascading failures and other instabilities.<sup>284</sup> The E-ISAC also provides additional support for utility preparedness in both nations.

However, Russia and other potential adversaries' increasingly sophisticated cyber capabilities pose challenges for protecting power flows between Canada and the United States, just as they do for electric service within each country individually.

Connectivity between US and Canadian power systems offers other benefits for protecting reliability against cyber and physical attacks. For example, as

<sup>276</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6-6.

<sup>277</sup> Stanley, *Mapping the U.S.-Canada Energy Relationship*, 9.

<sup>278</sup> Parfomak et al., *Cross-Border Energy Trade*, 34.

<sup>279</sup> "Work Continues on ITC Lake Erie Project," *Transmission Hub*.

<sup>280</sup> Vine, *Interconnected: Canadian and U.S. Electricity*, 9.

<sup>281</sup> NERC Steering Group, *Technical Analysis of Blackout*, 1.

<sup>282</sup> Governments of US and Canada, *Joint United States-Canada Electric Grid Security and Resilience Strategy*, 10.

<sup>283</sup> "North America," NERC. See also "Compliance - Québec," Northeast Power Coordinating Council; and "Electric Power Transmission Reliability Standards," Régie de l'énergie Québec.

<sup>284</sup> "Key Players," NERC.

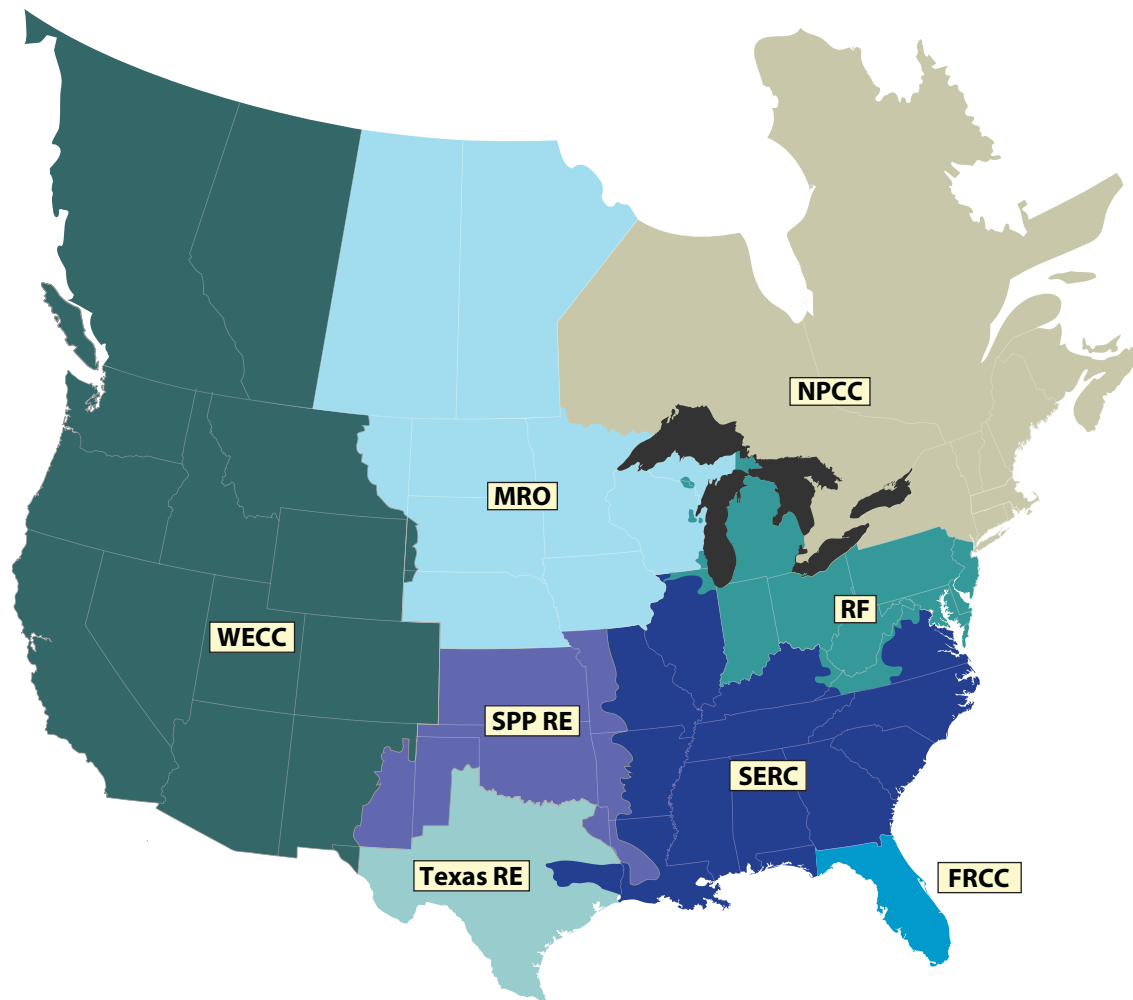


Figure 7. NERC Regional Entities across North America

new transmission lines increase this connectivity, electricity exported by Canada could become increasingly valuable when managing power imbalances in the United States and could make up for sudden shortfalls in the availability of US-generated power. However, we must assume that adversaries know this as well. To maximize the disruption to the US grid and the critical facilities that depend on it, attackers may strike the cross-border transmission lines that would otherwise help US grid owners and operators prevent cascading failures, uncontrolled separations, and other major reliability issues.

Adversaries may also attack grid assets that supply power to critical Canadian defense installations. The United States and Canada have a unique binational

defense system to protect their territories. The North American Aerospace Defense Command plays a vital role for both nations for aerospace warning, aerospace control, and maritime warning for North America.<sup>285</sup> The Canada-US Civil Assistance Plan also helps enable military members from one nation assist the other's armed forces in support of civilian authorities during emergencies.<sup>286</sup> Potential adversaries such as Russia may seek to degrade these binational military capabilities and operations by attacking defense critical electric infrastructure on

<sup>285</sup> "Canada-U.S. Defence Relationship," Department of National Defence and the Canadian Armed Forces.

<sup>286</sup> "Canada-U.S. Defence Relationship," Department of National Defence and the Canadian Armed Forces.



both sides of the border. US and Canadian officials and power companies should plan accordingly for mutual support in grid security emergencies.

### Specific Options for US–Canada Coordination

In addition to requiring US–Canada consultations before the secretary issues emergency orders, the FPA also states that FERC and the secretary “shall, in consultation with Canadian and Mexican authorities, develop protocols for the voluntary sharing of critical electric infrastructure information with Canadian and Mexican authorities and owners, operators and users of the bulk-power system outside the United States.”<sup>287</sup> Those initiatives provide a valuable starting point to build shared North American preparedness for grid security emergencies. However, much deeper collaboration is both possible and necessary, especially with Canada. Options for further analysis are described below.

**Consultative mechanisms, collaborative planning, and coordinated emergency operations.** The FPA does not specify how US officials would consult with their Canadian counterparts if the president declares a grid security emergency. Nor does it discuss whether the president would do so prior to making such a declaration. Exchanges between the US president and the prime minister of Canada would constitute the highest level of binational coordination. More detailed discussions about options for responding to incidents could also occur between the secretary of energy and the Canadian minister of national resources. That minister has the federal lead for electricity issues in Canada but lacks emergency authorities equivalent to those that the FPA grants to the secretary of energy.<sup>288</sup>

However, government coordination mechanisms will also need to include a broader array of participants. Global Affairs Canada and the US State Department might well be involved in any coordination of

binational grid emergency actions, just as they are in other emergency assistance mechanisms.<sup>289</sup> Coordination with state and provincial governments could also be helpful. The 1982 amendments to Canada’s Constitution Act (1867) explicitly recognized provinces’ and territories’ constitutional rights to manage electrical energy.<sup>290</sup> In particular, authority over electricity generation and transmission in Canada rests primarily with provincial governments.<sup>291</sup> It will be essential to account for these features of Canadian governance in building US–Canada consultative mechanisms.

The NERC alert system and other emergency coordination systems provide a solid basis for collaboration between US and Canadian utilities in grid security emergencies. However, the FPA does not address the question of how (and how much) information DOE officials should share with Canada on the issuance of emergency orders to US utilities. Given the deep integration of the US and Canadian grids, maximum sharing could help coordinate both countries’ emergency operations before, during, and after attacks. To facilitate such information sharing, DOE, Natural Resources Canada, and other relevant stakeholders can leverage existing US–Canadian mechanisms to protect sensitive information, supplemented as needed to support grid security emergency coordination.

The *Joint US-Canada Electric Grid Security and Resilience Strategy* (December 2016) provides a policy framework for building these coordination and information sharing mechanisms. The US and Canadian governments developed the strategy “to strengthen the security and resilience of the U.S. and Canadian electric grid from all adversarial, technological, and natural hazards and threats.”<sup>292</sup> The strategy calls for collaboration to protect system assets and

<sup>287</sup> 16 U.S.C. § 824o–1, (d)(5).

<sup>288</sup> “Roles and Responsibilities,” Natural Resources Canada.

<sup>289</sup> “Compendium,” Public Safety Canada.

<sup>290</sup> “Roles and Responsibilities,” Natural Resources Canada.

<sup>291</sup> “North America,” NERC.

<sup>292</sup> Governments of US and Canada, *US-Canada Electric Grid Security and Resilience Strategy*, 1.



critical functions in both nations so that the North American grid can “withstand and recover rapidly from disruptions.”<sup>293</sup> The strategy also emphasizes the need for collaboration to manage contingencies and enhance response and recovery efforts.<sup>294</sup> All of these features make the strategy a promising basis for creating the detailed collaborative mechanisms that grid security emergencies will require.

### **Protecting defense critical electric infrastructure.**

While the FPA facilitates the development of emergency orders to protect the flow of power to critical US defense installations, US–Canada coordination in grid security emergencies could also help strengthen power resilience for bases on both sides of the border. The Pacific Northwest exemplifies the potential benefits of such collaboration. Washington State hosts a number of vital installations, including Joint Base Kitsap on Puget Sound, which serves as the homeport for aircraft carriers, attack submarines, and other assets that would be needed for operations in the South China Sea and for other regional contingencies. Canadian Forces Base Esquimalt and other key Canadian installations are located less than one hundred miles away on Vancouver Island. Esquimalt is the second-largest military base in Canada and is home to Maritime Forces Pacific and Joint Task Force Pacific headquarters.<sup>295</sup> Coordinating US–Canada emergency plans to protect the flow of power to these installations could benefit the security of both nations.

The US–Canada Permanent Joint Board on Defense provides an ideal venue to explore such coordination options. Established in 1940 to discuss and advise on issues related to continental defense and security, the board has focused increasing attention on binational opportunities to strengthen critical infrastructure resilience. In 2011, the CEO of NERC led a

Permanent Joint Board on Defense discussion of how North American BPS emergency plans and coordination mechanisms could benefit US and Canadian national security. Natural Resources Canada and DOE have also participated in subsequent Permanent Joint Board on Defense meetings, along with the defense departments of both nations and critical infrastructure stakeholders. US and Canadian officials should consider using the board to facilitate industry–government discussions on opportunities to coordinate in grid security emergencies.

### **Coordination with Mexico and Beyond: Multinational Resilience against Grid Security Emergencies**

The US grid has much less connectivity with Mexican electric systems than with the Canadian grid. Southern California and a portion of Mexico’s Baja California have synchronous interconnections. Along the Mexico–Texas border, asynchronous interconnections also exist between the Electric Reliability Council of Texas (ERCOT) and Mexican utilities.<sup>296</sup> In 2017, Mexican and US officials agreed to nonbinding pledges to increase this connectivity in ways that would strengthen reliability on both sides of the border.<sup>297</sup>

The election of Mexican president Andrés Manuel López Obrador in July 2018 may lead to significant changes in that country’s energy policies.<sup>298</sup> Structural challenges will also slow efforts to increase US–Mexico grid integration, including repeated power shortages and major shortfalls in the functionality of the Mexican grid.<sup>299</sup> Nevertheless, it could be useful to expand discussions with industry and the incoming government on protecting grid reliability against cyber and physical threats.

<sup>293</sup> Governments of US and Canada, *US–Canada Electric Grid Security and Resilience Strategy*, 12.

<sup>294</sup> Governments of US and Canada, *US–Canada Electric Grid Security and Resilience Strategy*, 11.

<sup>295</sup> “Maritime Forces Pacific,” Royal Canadian Navy.

<sup>296</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6–4.

<sup>297</sup> “Increasing Electricity Cooperation in North America,” DOE.

<sup>298</sup> Kissane and Medina, “Energy Aftershocks.”

<sup>299</sup> DOE, *Quadrennial Energy Review: Second Installment*, 6–13.

Building grid security emergency coordination mechanisms beyond North America would also be helpful. As noted earlier, attacks on the US grid are most likely to occur in the context of an intense, escalating regional crisis in the Baltics, Northeast Asia, or some other area where US allies and critical security interests are at risk. In particular, adversaries may seek to inflict blackouts that could disrupt the deployment of US forces to the crisis zone. But we should also expect that US allies in the region will suffer attacks on their own grids, aimed at disrupting their ability to conduct combined operations with the United States and deliver electricity to US bases on their territories.

NATO's 2018 Locked Shields exercise focused on building alliance-wide preparedness for cyber and physical attacks against energy and communications systems.<sup>300</sup> In future exercises, allies might explore how to jointly determine whether grid attacks are potentially imminent and coordinate on the implementation of conservative operations across NATO member countries. The United States might explore equivalent opportunities for collaboration with Japan, South Korea, Australia, New Zealand, and other security partners. Existing treaty commitments, including those under Article V of NATO's founding treaty, will provide a starting point to meet our shared grid resilience challenges.<sup>301</sup>

## Playing Defense in Cyberwarfare: Doctrine, Integrated Planning, and Benefits for Deterrence

Utility leaders are urging the federal government to do more to assist them in deterring and defeating attacks on the grid. Their calls come at a perfect time. Administration officials have opened the door to new forms of operational collaboration between industry and government, including "collective

defense" during cyber attacks.<sup>302</sup> This report examines an especially significant option to expand their collaboration: coordinating the implementation of emergency orders with DOD operations to halt attacks at their source.

Deeper operational partnerships can also help meet underlying challenges for cyber deterrence. A number of cybersecurity analysts argue that deterrence by denial is impractical in cyberspace because offensive cyber capabilities are so much stronger than cyber defenses, and because cyber warfare will be very different from conventional conflicts. Analysts also warn that the United States lives in a cyber "glass house": given the vulnerability of the power grid and other infrastructure systems, the president cannot credibly threaten to use cyber weapons to defend US allies and interests. Improving preparedness for grid security emergencies can help address these concerns and support ongoing reassessments of US strategies for deterrence.

## Unity of Effort in Defensive Operations at Home and Abroad

Tom Fanning, CEO of Southern Company (one of the largest power companies in the United States), notes that he and other infrastructure owners and operators face a major constraint on their ability to defend their systems: "I can't fight back."<sup>303</sup> In theory, blunting attacks at their source could greatly ease the scale and severity of the threats that utilities will need to counter. In practice, integrating grid security emergency operations with measures to suppress enemy attacks would entail major policy and technical obstacles.

Power companies should not be responsible for striking enemies' offensive cyber infrastructure during grid security emergencies. The US government is the sole actor with the prerogative to engage in techniques such as "hacking back" that

<sup>300</sup> Cowan, "Locked Shields 2018."

<sup>301</sup> "The North Atlantic Treaty," NATO.

<sup>302</sup> Nielsen, *National Cybersecurity Summit Keynote Speech*.

<sup>303</sup> Smith, "U.S. Officials Push New Penalties."

involve operations to disrupt or destroy an attacker's system.<sup>304</sup> Moreover, even if power companies gained legal authority to fight back against adversaries, their technical capacity to do so would be dwarfed by the capabilities possessed by US Cyber Command and other US government organizations.

Efforts to integrate defensive operations at home and abroad should rest on the comparative advantages of industry and government. BPS entities and other components of the electricity subsector are best positioned to defend their systems from within, assisted by DOE and other government partners. Operations abroad to halt attacks on the grid should remain the exclusive purview of government agencies, supported by industry assistance to gather malware samples and facilitate attack attribution. Based on this division of labor, government and industry leaders could explore whether and how to strengthen unity of effort for the full scope of defensive operations within the United States and beyond.

Secretary of homeland security Kirstjen Nielsen has called for the adoption of a "collective defense" posture that might include such expanded partnerships. Under the collective defense model, industry and government would collaborate to act on threat indicators and "respond more quickly and effectively to incidents."<sup>305</sup> The most familiar realm of operational collaboration lies in government support to help utilities detect, characterize, and eradicate malware on their systems. DHS is strengthening the National Cybersecurity and Communications Integration Center's ability to provide such assistance.<sup>306</sup> State National Guard organizations can also support post-cyber attack power restoration within the larger context of the industry's Cyber Mutual Assistance system.<sup>307</sup> However, in a cyber strike against the

United States, DOD will require many of these same guard personnel to protect the department's networks, conduct cyber operations against the attacker, and carry out other federal missions.<sup>308</sup> Power companies and government agencies will need to continue clarifying whether and how specific National Guard assets can help meet utility requests for assistance; existing doctrine and procedures for providing defense support to civil authorities offer a solid basis to advance those discussions.

In contrast, coordinating industry grid protection measures with government operations to suppress attacks would extend collective defense into uncharted territory. The command vision for US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, offers a starting point to examine how engaging against malicious cyber actors might help protect utilities. The document states that the United States must "increase resiliency, defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors to generate continuous tactical, operational, and strategic advantage." To do so, DOD "is building the operational expertise and capacity to meet growing cyberspace threats and stop cyber aggression before it reaches our networks and systems."<sup>309</sup>

Forward defense operations could respond to and help counter adversary efforts to implant malware on utility networks. Should such operations also help power companies protect their systems if the president declares that an attack is imminent? As senator Mike Rounds frames the question: "If someone is going to shoot an arrow at you, do you shoot the archer before he shoots the arrow?"<sup>310</sup>

US Cyber Command's vision statement does not directly address this possibility. However, each phase of grid security emergencies will likely offer

<sup>304</sup> GWU, *Into the Gray Zone*, 25.

<sup>305</sup> Nielsen, *National Cybersecurity Summit Keynote Speech*.

<sup>306</sup> Marks, "DHS Stands Up New Cyber Risk Center."

<sup>307</sup> Crowe, "National Guard Preparing"; and Puryear, "91st Cyber Brigade Activated."

<sup>308</sup> DOD, *Cyber Strategy*, 4.

<sup>309</sup> US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 4–5.

<sup>310</sup> Bordelon, "Rounds Is Ready."

a different mix of risks and rewards for combining domestic and forward defense operations. For example, if the president determines that an attack on the grid is imminent, the secretary might issue orders for conservative operations to bolster grid defenses at the same moment that forward defense operations disrupted enemy cyber infrastructure poised to launch the strike. But assessments that an attack is imminent may turn out to be wrong. No-regrets orders for conservative operations are valuable precisely because using them will entail few consequences if warning indicators turn out to be false. Preattack forward defense operations could start a cyberwar that might not otherwise have occurred.

The United States can avoid such risks by waiting until attacks on the grid are under way before striking the enemy's offensive infrastructure. However, developing the technical capabilities to identify and disrupt the cyber infrastructure being used in an attack could prove challenging. Moreover, it is not clear whether integrating plans for home and away operations would offer significant benefits, as opposed to relying on utilities and government agencies to conduct those two types of operations independently.

US Cyber Command has opened the door to building new types of partnerships with the electricity subsector. The command has called for measures to "deepen and operationalize" collaboration between the private sector, the armed services, and other command partners.<sup>311</sup> As those efforts go forward with the electricity subsector and DOE, exploring options for collective defense (and clarifying the dangers they might present) should be a prime focus for analysis.

### **Maximizing Industry Contributions to Cyber Deterrence by Denial**

The *National Security Strategy* emphasizes that rather than rely on threats of cost imposition alone

to deter enemy attacks, the United States will also strengthen deterrence by denial. This report has examined how grid security emergency orders and implementation plans can raise adversaries' doubts as to whether they can achieve their objectives. But strengthening this form of deterrence will also entail underlying challenges.

Many cybersecurity analysts believe that offensive cyber capabilities are vastly stronger than defenses against them, and that this preeminence creates destabilizing incentives for adversaries to strike first when conflicts loom.<sup>312</sup> Unless measures to strengthen grid resilience can help weaken the dominance of offense over defense in the cyber realm, deterrence by denial will remain difficult to accomplish against highly capable adversaries.

However, today's offensive dominance stems in part from historical factors that are rapidly changing. The interconnected grid evolved decades ago when no cyber threat existed to drive protective measures. Moreover, as utilities began incorporating computer-assisted controls, sensors, and operating technology systems, few of these companies accounted for the risk that cyber threats to their systems would escalate so rapidly. As noted in this report, utilities are advancing a wide array of technical initiatives and fallback operational plans to counter and (ideally) stay ahead of adversaries' capabilities. In addition, regulatory bodies across the nation are increasingly willing to enable companies to recover costs for cyber resilience.

The current preeminence of offense over defense also reflects organizational factors. Rebecca Slayton has found that historically, "the success of offense is largely the result of a poorly managed defense."<sup>313</sup> The skills of the individuals employing cyber weapons and defensive tools, and the effectiveness with which

<sup>311</sup> US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 8.

<sup>312</sup> For a review of this "offense-dominant" literature, and the smaller set of works opposing it, see Slayton, "What Is the Cyber Offense-Defense Balance?," 72.

<sup>313</sup> Slayton, "What Is the Cyber Offense-Defense Balance?," 87.



these practitioners are managed and organized, have an enormous impact on the outcome of cyber engagements. Slayton notes that the importance of organization for cyber defense is implicit in discussions of the need for better public-private partnerships and information sharing. What has been missing, however, are efforts to make such partnerships *operational* and create unity of effort in government-industry defense actions when adversaries strike. That is precisely the gap that DOE and its industry partners can fill by developing grid security emergency orders and advancing all of the other collaborative initiatives necessary to make those orders effective.

Improved partnerships and technical capabilities to protect the grid cannot by themselves make defense preeminent. To further rebalance offense and defense in cyberspace, resilience initiatives will be necessary across all critical infrastructure sectors, as well as a host of other measures to facilitate the command, control, and coordination of public-private defensive operations. But building preparedness for grid security emergencies will be vital for that broader effort. Moreover, establishing defensive primacy is not necessary to facilitate deterrence by denial. As defined by the *National Security Strategy*, deterrence by denial functions by creating doubt in our adversaries that they can achieve their objectives.<sup>314</sup> DOE and its partners should develop grid security emergency orders that (perhaps in conjunction with forward defense operations) can make adversaries less likely to attack, even if defensive dominance remains out of reach.

Strengthening grid resilience can also support the broader reassessment of the US deterrence posture that is now under way. Robert Strayer, the State Department's deputy assistant secretary for cyber and international communications and information policy, notes that the increasing severity of threats to

US infrastructure is forcing "an evolution in the US government's thinking about how to deter malicious cyber actors."<sup>315</sup> In conventional warfare, deterrence by denial functions by making it physically difficult for adversaries to achieve their objectives and by raising enemy forces' costs of taking their targets.<sup>316</sup> Cyberwarfare will not entail the same sorts of attrition of enemy forces that occurs in battles with tanks, fighter aircraft, and other conventional weapons. The Trump and Obama administrations have redefined deterrence by denial to better fit the characteristics of cyberspace. The unique features of cyber conflict will require continued rethinking of how the United States can strengthen deterrence in the years to come. As utilities and government agencies build resilience for grid security emergencies, new opportunities will emerge to influence adversaries' perceived costs and benefits of attack. The United States should continue to refine its deterrence posture to capitalize on these improvements.

### Escaping the "Glass House" Syndrome

The president may need the ability to use cyber weapons against foreign targets to help resolve crises on terms favorable to the United States. The *DOD Cyber Strategy* (April 2015) states that:

There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an

<sup>314</sup> White House, *National Security Strategy*, 13.

<sup>315</sup> Smith, "U.S. Officials Push New Penalties."

<sup>316</sup> For definitions of classic deterrence by denial derived from conventional warfare, see Gerson, "Conventional Deterrence"; and Mitchell, "The Case for Deterrence by Denial." For an analysis of how that definition differs from that used by the Trump administration, see Fischerkeller and Harknett, "Deterrence Is Not a Credible Strategy."



ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests.<sup>317</sup>

However, any such operations against an adversary's cyber infrastructure would risk retaliatory strikes against the United States—including, potentially, attacks on the grid. Senator Thom Tillis (R-NC), a member of the Senate Armed Service Committee, emphasizes that the United States is living in “a big glass house.”<sup>318</sup> If US infrastructure owners and operators cannot defend their systems against attack, the president may be reluctant to use cyber weapons abroad, even if doing so might otherwise offer enormous benefits for conflict termination. In short: US leaders may be self-deterred from taking actions that they may need to employ. Developing emergency orders and implementation plans to protect grid reliability could reduce these glass house constraints and widen the range of options available for the president to protect US interests.

Improving grid defenses could also help strengthen the credibility of US commitments to defend key allies. Former US defense and intelligence officials have proposed that the United States and other high-cyber-capability NATO allies provide extended deterrence against cyber attacks for less capable alliance members.<sup>319</sup> But glass house concerns would call into question the credibility such commitments. Measures to strengthen grid resilience could help convince adversaries that the United States is willing to help allies respond to cyber attacks on their infrastructure.

Yet, nothing requires the United States to respond to such attacks with cyber weapons alone. On the contrary: the *National Security Strategy* and other policy documents leave open the possibility that

if cyber attacks at home or abroad are sufficiently severe, the United States will respond with conventional or even nuclear weapons. James Lewis notes that “opponents are keenly aware that launching catastrophe brings with it immense risk of receiving catastrophe in return,” and will surely weigh that risk given “the immense capacity of the United States to inflict punishment” on attackers.<sup>320</sup> Emergency orders to protect the flow of power to defense installations can and should reinforce the certainty of that punishment.

But any first use of cyber weapons by the United States would entail escalatory dangers as well. If the United States were to initiate the use of destructive cyber weapons to defend US allies and interests, potential adversaries such as Russia could respond with conventional or nuclear forces. Moreover, conflicts that begin with the large-scale use of cyber weapons could also spiral out of control in ways that neither side desires or anticipates.<sup>321</sup> These escalatory risks must be in the forefront of calculations on whether and how to engage in cyber warfare. Indeed, as government agencies partner with power companies to build resilience for grid security emergencies, deterring such conflicts and reducing the likelihood of cyberwarfare should always be our prime objective.

<sup>317</sup> DOD, *Cyber Strategy*, 5.

<sup>318</sup> Schwartz, “Sen. Tillis: We Are Living in a Glass House.” For additional analysis of the glass house syndrome and its effects on constraining US options, see Miller, “Cyber Deterrence”; and Rosenbach, “Living in a Glass House.”

<sup>319</sup> Kramer, Butler, and Lotrionte, *Cyber, Extended Deterrence, and NATO*, 1.

<sup>320</sup> Lewis, *Rethinking Cybersecurity*, 9, 29. The author also argues that even if attacks on the grid occur, they would be unlikely to achieve the strategic effects that adversaries will seek, further reducing the likelihood of such attacks (see pp. 21 and 24–26).

<sup>321</sup> Danzig, *Surviving on a Diet of Poisoned Fruit*, 25; Lin, “Escalation Dynamics,” 52; and Miller and Fontaine, *A New Era*, 18–20.

## Bibliography

- 6 U.S.C. § 124l. <https://www.law.cornell.edu/uscode/text/6/124l>.
- 15 U.S.C. § 3361. <https://www.law.cornell.edu/uscode/text/15/3361>.
- 15 U.S.C. § 3363. <https://www.law.cornell.edu/uscode/text/15/3363>.
- 15 U.S.C. § 3364. <https://www.law.cornell.edu/uscode/text/15/3364>.
- 16 U.S.C. § 824a. <https://www.law.cornell.edu/uscode/text/16/824a>.
- 16 U.S.C. § 824o. <https://www.law.cornell.edu/uscode/text/16/824o>.
- 16 U.S.C. § 824o–1. [https://www.law.cornell.edu/uscode/text/16/824o–1](https://www.law.cornell.edu/uscode/text/16/824o-1).
- 18 CFR 388.113. <https://www.law.cornell.edu/cfr/text/18/388.113>.
- 47 U.S.C. § 606. <https://www.law.cornell.edu/uscode/text/47/606>.
- 50 U.S.C. Appendix §2071(c). <https://law.justia.com/codes/us/2001/title50/app/defensepr/sec2071/>.
- “About Alerts.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/pa/rrm/bpsa/Pages/About-Alerts.aspx>.
- “About NERC.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/AboutNERC/Pages/default.aspx>.
- “About NSTAC.” DOS (US Department of State). Last published June 20, 2016. <https://www.dhs.gov/about-nstac>.
- “About 60% of the U.S. Electric Power Supply Is Managed by RTOs.” US Energy Information Administration. April 4, 2011. <https://www.eia.gov/todayinenergy/detail.php?id=790>.
- “Alert (ICS-ALERT-14-281-01E): Ongoing Sophisticated Malware Campaign Compromising ICS (Update E).” ICS-CERT. Originally released December 10, 2014, last revised December 9, 2016. <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B>.
- “Alert (IR-ALERT-H-16-056-01): Cyber-Attack against Ukrainian Critical Infrastructure.” ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). February 25, 2016. <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>.
- “Alert (TA17-163A): CrashOverride Malware.” US-CERT (US Computer Emergency Readiness Team). June 12, 2017. <https://www.us-cert.gov/ncas/alerts/TA17-163A>.
- “Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors.” US-CERT (US Computer Emergency Readiness Team). October 20, 2017. <https://www.us-cert.gov/ncas/alerts/TA17-293A>.
- “Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.” US-CERT (US Computer Emergency Readiness Team). March 15, 2018. <https://www.us-cert.gov/ncas/alerts/TA18-074A>.

- ASD(EI&E) (Office of the Assistant Secretary of Defense for Energy, Installations, and Environment). *Annual Energy Management and Resilience (AEMR) Report Fiscal Year 2016*. Washington, DC: DOD, July 2017. <https://www.acq.osd.mil/EIE/Downloads/IE/FY%202016%20AEMR.pdf>.
- Assante, Michael, and Robert M. Lee. *The Industrial Control System Cyber Kill Chain*. Bethesda, MD: SANS Institute, October 2015. <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>.
- “Automated Indicator Sharing (AIS).” US-CERT (US Computer Emergency Readiness Team). n.d. <https://www.us-cert.gov/ais>.
- Banham, Russ. “DDoS Attacks Evolve to Conscript Devices onto the IoT.” *Forbes*, February 4, 2018. <https://www.forbes.com/sites/centurylink/2018/02/04/ddos-attacks-evolve-to-conscript-devices-onto-the-iot/#4b5a43a86aaa>.
- Barnes, Julian E. “‘Warning Lights Are Blinking Red,’ Top Intelligence Officer Says of Russian Attacks.” *New York Times*, July 13, 2018. <https://www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html>.
- Blue Ribbon Study Panel on Biodefense (Hudson Institute). *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts—A Bipartisan Report of the Blue Ribbon Study Panel on Biodefense*. Washington, DC: Hudson Institute, October 2015. <http://www.biodefensestudy.org/a-national-blueprint-for-biodefense>.
- Bordelon, Brendan. “Rounds Is Ready to Lead New Senate Cybersecurity Subcommittee.” *Morning Consult*, February 1, 2017. <https://morningconsult.com/2017/02/01/rounds-ready-lead-new-senate-cybersecurity-subcommittee/>.
- Brown, Jared T., and Daniel H. Else. *The Defense Production Act of 1950: History, Authorities, and Reauthorization*. Washington, DC: Congressional Research Service, July 28, 2014. <https://fas.org/sgp/crs/natsec/R43118.pdf>.
- “The Canada-U.S. Defence Relationship.” Department of National Defence and the Canadian Armed Forces. December 4, 2014, last modified February 10, 2015. <http://www.forces.gc.ca/en/news/article.page?doc=the-canada-u-s-defence-relationship/hob7hd8s>.
- Cherepanov, Anton, and Robert Lipovsky. “Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet.” *WeLiveSecurity* (ESET Blog), June 12, 2017. <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>.
- “Compendium of U.S.-Canada Emergency Management Assistance Mechanisms.” Public Safety Canada. October 2016, last modified March 28, 2018. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/cmpndm-ntdstts-cnd-2016/index-en.aspx>.
- “Compliance - Québec.” Northeast Power Coordinating Council. n.d. <https://www.npcc.org/Compliance/Quebec/Forms/Public%20List.aspx>.
- Cowan, Gerrard. “Locked Shields 2018 Practises for Large-Scale Cyber Incident.” *Jane’s 360*, April 29, 2018. <http://www.janes.com/article/79652/locked-shields-2018-practises-for-large-scale-cyber-incident>.

- Crowe, Greg. "National Guard Preparing to Defend Cyberspace for States." *Federal News Radio*, April 16, 2018. <https://federalnewsradio.com/cyber-exposure/2018/04/national-guard-preparing-to-defend-cyberspace-for-states/>.
- "Cybersecurity." American Gas Association. n.d. <https://www.aga.org/safety/security/cybersecurity/>.
- "The Cyber Threat Framework." ODNI (Office of the Director of National Intelligence). n.d. <https://www.dni.gov/index.php/cyber-threat-framework>.
- Danzig, Richard. *Catastrophic Bioterrorism—What Is to Be Done?* Washington, DC: Center for Technology and National Security Policy, August 2003. [http://www.response-analytics.org/images/Danzig\\_Bioterror\\_Paper.pdf](http://www.response-analytics.org/images/Danzig_Bioterror_Paper.pdf).
- . *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*. Washington, DC: Center for a New American Security, July 2014. [https://s3.amazonaws.com/files.cnas.org/documents/CNAS\\_PoisonedFruit\\_Danzig.pdf](https://s3.amazonaws.com/files.cnas.org/documents/CNAS_PoisonedFruit_Danzig.pdf).
- Defense Science Board. *Task Force on Cyber Deterrence*. Washington, DC: DOD, February 2017. [https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport\\_02-28-17\\_Final.pdf](https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf).
- DHS (US Department of Homeland Security). *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. Washington, DC: DHS, December 17, 2003. <https://www.dhs.gov/homeland-security-presidential-directive-7>.
- . *National Cyber Incident Response Plan*. Washington, DC: DHS, December 2016. [https://www.us-cert.gov/sites/default/files/ncirp/National\\_Cyber\\_Incident\\_Response\\_Plan.pdf](https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf).
- . *National Response Framework*. 3rd ed. Washington, DC: DHS, June 2016. [https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National\\_Response\\_Framework3rd.pdf](https://www.fema.gov/media-library-data/1466014682982-9bcf8245ba4c60c120aa915abe74e15d/National_Response_Framework3rd.pdf).
- . *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: DHS, 2013. <https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf>.
- . *Power Outage Incident Annex to the Response and Recovery Federal Interagency Operational Plans: Managing the Cascading Impacts from a Long-Term Power Outage*. Washington, DC: DHS, June 2017. <https://www.fema.gov/media-library/assets/documents/154058>.
- . *Strategy for Protecting and Preparing the Homeland against the Threats of Electromagnetic Pulse and Geomagnetic Disturbances*. Washington, DC: DHS, forthcoming.
- . *U.S. Department of Homeland Security Cybersecurity Strategy*. Washington, DC: DHS, May, 15, 2018. [https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy\\_1.pdf](https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf).
- DiSavino, Scott, and David Sheppard. "ConEd Cuts Power to Part of Lower Manhattan Due to Sandy." *Reuters*, October 29, 2012. <https://www.reuters.com/article/us-storm-sandy-conedison/coned-cuts-power-to-part-of-lower-manhattan-due-to-sandy-idUSBRE89S1CP20121030>.

- DOD (US Department of Defense). *Department of Defense Manual 3020.45*. Washington, DC: DOD, last updated May 23, 2017. <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302045V5p.pdf>.
- . *DoD Cybersecurity Discipline Implementation Plan*. Washington, DC: DOD, amended February 2016. <http://dodcio.defense.gov/Portals/0/Documents/Cyber/CyberDis-ImpPlan.pdf>.
- . *DOD Cyber Strategy*. Washington, DC: DOD, April 2015. [https://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final\\_2015\\_DoD\\_CYBER\\_STRATEGY\\_for\\_web.pdf](https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf).
- . *DoD Directive 3020.40: Mission Assurance (MA)*. Washington, DC: DOD, November 29, 2016. [http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040\\_dodd\\_2016.pdf](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040_dodd_2016.pdf).
- . *Mission Assurance Strategy*. Washington, DC: DOD, April 2012. [http://policy.defense.gov/Portals/11/Documents/MA\\_Strategy\\_Final\\_7May12.pdf](http://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf).
- DOE (US Department of Energy). “Grid Security Emergency Orders: Procedures for Issuance (RIN 1901–AB40).” *Federal Register* 83, no. 7 (2018): 1176. <https://www.federalregister.gov/documents/2018/01/10/2018-00259/grid-security-emergency-orders-procedures-for-issuance>.
- . *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*. Version 1.1. Washington, DC: DOE, February 2014. <https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf>.
- . *Electromagnetic Pulse Resilience Action Plan*. Washington, DC: DOE, January 2017. <https://www.energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf>.
- . “Energy Priorities and Allocations System Regulations (RIN 1901–AB28).” *Federal Register* 76, no. 111 (2011): 33615. <https://www.gpo.gov/fdsys/pkg/FR-2011-06-09/pdf/2011-14282.pdf>.
- . *Multiyear Plan for Energy Sector Cybersecurity*. Washington, DC: DOE, March 2018. [https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20\\_0.pdf](https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf).
- . *Quadrennial Energy Review—Transforming the Nation’s Electricity System: The Second Installment of the QER*. Washington, DC: DOE, January 2017. <https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf>.
- . *Staff Report to the Secretary on Electricity Markets and Reliability*. Washington, DC: DOE, August 2017. [https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability\\_0.pdf](https://www.energy.gov/sites/prod/files/2017/08/f36/Staff%20Report%20on%20Electricity%20Markets%20and%20Reliability_0.pdf).
- . *Strategic Transformer Reserve: Report to Congress*. Washington, DC: DOE, March 2017. <https://energy.gov/sites/prod/files/2017/04/f34/Strategic%20Transformer%20Reserve%20Report%20-%20FINAL.pdf>.
- “DOE’s Use of Federal Power Act Emergency Authority.” DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/services/electricity-policy-coordination-and-implementation/other-regulatory-efforts/does-use>.



- DOS (US Department of State). *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats*. Washington, DC: DOS, May 31, 2018. <https://www.state.gov/documents/organization/282253.pdf>.
- Dougherty, Jon. “Biggest U.S. Power Grid Operator Suffers Thousands of Attempted Cyber Attacks per Month.” *Forward Observer*, August 28, 2017. <https://forwardobserver.com/2017/08/biggest-u-s-power-grid-operator-suffers-thousands-of-attempted-cyber-attacks-per-month/>.
- Douris, Constance. “DARPA Research Leads Grid Security Solutions.” *The Buzz* (blog), *National Interest*, January 12, 2017. <http://nationalinterest.org/blog/the-buzz/darpa-research-leads-grid-security-solutions-19044>.
- Dragos, Inc. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations*. Hanover, MD: Dragos, June 13, 2017. <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>.
- EEI (Edison Electric Institute). “Comments of the Edison Electric Institute.” In *Response to Grid Security Emergency Orders: Procedures for Issuance (RIN 1901-AB40)*. February 6, 2017.
- . *Understanding the Electric Power Industry’s Response and Restoration Process*. Washington, DC: EEI, October 2016. [http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA\\_101FINAL.pdf](http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf).
- EIS Council (Electric Infrastructure Security Council). *E-PRO Handbook II: Volume 1—Fuel*. Washington, DC: EIS Council, 2016. [https://www.eiscouncil.org/App\\_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf](https://www.eiscouncil.org/App_Data/Upload/149e7a61-5d8e-4af3-bdbf-68dce1b832b0.pdf).
- . *E-PRO Handbook III: Black Sky Cross-Sector Coordination and Communication*. Washington, DC: EIS Council, June 2018. [https://www.eiscouncil.org/EPRO\\_Books.aspx](https://www.eiscouncil.org/EPRO_Books.aspx).
- E-ISAC (Electricity Information Sharing and Analysis Center) and SANS-ICS. *Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case*. Washington, DC: NERC, March 2016. [https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_18Mar2016.pdf](https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf).
- “Electricity Information Sharing and Analysis Center.” NERC (North American Electric Reliability Corporation). n.d. <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>.
- “Electric Power Transmission Reliability Standards Compliance Monitoring and Enforcement.” Régie de l’énergie Québec. n.d. <http://www.regie-energie.qc.ca/en/audiences/NormesFiabiliteTransportElectricite/NormesFiabilite.html>.
- “Emergency Communications.” DHS (US Department of Homeland Security). Last published June 26, 2018. <https://www.dhs.gov/topic/emergency-communications>.
- Energy Policy Act of 2005. Public Law 109-58. *U.S. Statutes at Large* 119 (2005): 942–943. <https://www.gpo.gov/fdsys/pkg/STATUTE-119/pdf/STATUTE-119.pdf>.
- “Energy Sector Cybersecurity Preparedness.” DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness-0>.

- EPRI (Electric Power Research Institute). *Electromagnetic Pulse and Intentional Electromagnetic Interference (EMI) Threats to the Power Grid: Characterization of the Threat, Available Countermeasures, and Opportunities for Technology Research*. Report 3002000796. Palo Alto, CA: EPRI, December 2013. <https://publicdownload.epri.com/PublicDownload.svc/product=000000003002000796/type=Product>.
- . *High-Altitude Electromagnetic Pulse Effects on Bulk-Power Systems: State of Knowledge and Research Needs*. Report 3002008999. Palo Alto, CA: EPRI, September 2016. <https://www.epri.com/#/pages/product/000000003002008999/?lang=en>.
- ESCC (Electricity Subsector Coordinating Council). *Electricity Sub-Sector Coordinating Council Charter*. Washington, DC: DHS, August 5, 2013. <https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf>.
- “ESCC: Electricity Subsector Coordinating Council.” ESCC (Electricity Subsector Coordinating Council). January 2018. <http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8>.
- “The ESCC’s Cyber Mutual Assistance Program.” ESCC (Electricity Subsector Coordinating Council). January 2018. <http://www.electricitysubsector.org/CMA/Cyber%20Mutual%20Assistance%20Program%20One-Pager.pdf?v=1.1>.
- FEMA (US Federal Emergency Management Agency). *2017 Hurricane Season FEMA After-Action Report*. Washington, DC: FEMA, July 12, 2018. <https://www.fema.gov/media-library/assets/documents/167249>.
- FERC (Federal Energy Regulatory Commission). *Cyber Security Incident Reporting Reliability Standards*. 161 FERC ¶ 61,291. December 21, 2017. <https://www.ferc.gov/whats-new/comm-meet/2017/122117/E-1.pdf>.
- . *Extraordinary Expenditures Necessary to Safeguard National Energy Supplies, Statement of Policy*. 96 FERC ¶ 61,299. September 14, 2011.
- . *Grid Resilience in Regional Transmission Organizations and Independent System Operators*. 162 FERC ¶ 61,256. 2018. <https://www.ferc.gov/CalendarFiles/20180320102618-AD18-7-000.pdf>.
- . *Order Authorizing Acquisition and Disposition of Jurisdictional Facilities*. 163 FERC ¶ 61,005. April 3, 2018. <https://www.ferc.gov/CalendarFiles/20180403165704-EC18-32-000.pdf>.
- . *Order Granting Approvals in Connection with the Dissolution of the Southwest Power Pool Regional Entity*. 163 FERC ¶ 61,094. May 4, 2018. <https://www.ferc.gov/CalendarFiles/20180504141902-RR18-3-000.pdf>.
- . *Policy Statement on Matters Related to Bulk Power System Reliability*. 107 FERC ¶ 61,052. April 19, 2004. <https://www.ferc.gov/whats-new/comm-meet/041404/E-6.pdf>.
- . *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*. Order No. 833. 157 FERC ¶ 61,123. November 17, 2016. <https://www.ferc.gov/whats-new/comm-meet/2016/111716/E-4.pdf>.
- . *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*. Order No. 833-A. 163 FERC ¶ 61,125. May 17, 2018. <https://www.ferc.gov/whats-new/comm-meet/2018/051718/E-2.pdf>.

- . *Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events*. 156 FERC ¶ 61,215. September 22, 2016. <https://www.ferc.gov/whats-new/comm-meet/2016/092216/E-4.pdf>.
- . *Revision to Electric Reliability Organization Definition of Bulk Electric System*. Order No. 743. 133 FERC ¶ 61,150. November 18, 2010. <https://www.ferc.gov/whats-new/comm-meet/2010/111810/E-2.pdf>.
- . *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*. Order No. 773-A. 143 FERC ¶ 61,053. April 18, 2013. <https://www.ferc.gov/whats-new/comm-meet/2013/041813/E-9.pdf>.
- FERC (Federal Energy Regulatory Commission) and NERC (North American Electric Reliability Corporation). *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans*. Washington, DC: FERC, January 2016. <https://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf>.
- . *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans—Further Joint Study Report: Planning Restoration Absent SCADA or EMS (PRASE)*. Washington, DC: FERC, June 2017. <https://www.ferc.gov/legal/staff-reports/2017/06-09-17-FERC-NERC-Report.pdf>.
- . *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans—Recommended Study: Blackstart Resources Availability (BRAv)*. Washington, DC: FERC, May 2018. <https://www.ferc.gov/legal/staff-reports/2018/bsr-report.pdf>.
- Fischerkeller, Michael P., and Richard J. Harknett. “Deterrence Is Not a Credible Strategy for Cyberspace.” *Orbis* 61, no. 3 (2017): 381–393. <https://www.sciencedirect.com/science/article/pii/S0030438717300431>.
- Fixing America’s Surface Transportation Act, Public Law 114-94. *U.S. Statutes at Large* 129 (2015): 1773–1774. <https://www.congress.gov/114/plaws/publ94/PLAW-114publ94.pdf>.
- Frankel, Alison. “Can Customers Sue Power Companies for Outages? Yes, but It’s Hard to Win.” *Reuters* (blog), November 9, 2012. <http://blogs.reuters.com/alison-frankel/2012/11/09/can-customers-sue-power-companies-for-outages-yes-but-its-hard-to-win/>.
- Galloway, T. J., Sr. “Advancing Reliability and Resilience of the Grid.” Comments presented at the FERC Reliability Technical Conference, Washington, DC, July 31, 2018. <https://www.ferc.gov/CalendarFiles/20180731084251-Galloway,%20North%20American%20Transmission%20Forum.pdf>.
- Gerson, Michael S. “Conventional Deterrence in the Second Nuclear Age.” *Parameters* 39 (Autumn 2009): 32–48. <https://ssi.armywarcollege.edu/pubs/parameters/articles/09autumn/gerson.pdf>.
- Governments of the US and Canada. *Joint United States-Canada Electric Grid Security and Resilience Strategy*. Washington, DC: The White House, December 2016. [https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint\\_US\\_Canada\\_Grid\\_Strategy\\_06Dec2016.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Joint_US_Canada_Grid_Strategy_06Dec2016.pdf).
- GWU (George Washington University) Center for Cyber and Homeland Security. *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats*. Washington, DC: GWU, October 2016. <https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf>.
- Healy, Jason. *The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities*. SSRN, June 2016. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2836206](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836206).

- Homeland Security Advisory Council. *Final Report of the Cybersecurity Subcommittee: Part I—Incident Response*. Washington, DC: DOS, June 2016. <https://www.hsd.org/?view&did=794271>.
- ICF. *Assessment of Large Power Transformer Risk Mitigation Strategies*. Fairfax, VA: ICF, October 2016. <https://www.energy.gov/sites/prod/files/2017/01/f34/Assessment%20of%20Large%20Power%20Transformer%20Risk%20Mitigation%20Strategies.pdf>.
- . *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*. Fairfax, VA: ICF, June 2016. <https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf>.
- “Increasing Electricity Cooperation in North America.” DOE (US Department of Energy). January 11, 2017. <https://www.energy.gov/policy/articles/increasing-electricity-cooperation-north-america>.
- INL (Idaho National Laboratory). *Strategies, Protections, and Mitigations for the Electric Grid from Electromagnetic Pulse Effects*. Idaho Falls, IN: INL, January 2016. <https://inldigitallibrary.inl.gov/sites/STI/STI/INL-EXT-15-35582.pdf>.
- ISO-NE (ISO New England). *Operational Fuel-Security Analysis*. Holyoke, MA: ISO-NE, January 17, 2018. [https://www.iso-ne.com/static-assets/documents/2018/01/20180117\\_operational\\_fuel-security\\_analysis.pdf](https://www.iso-ne.com/static-assets/documents/2018/01/20180117_operational_fuel-security_analysis.pdf).
- . “Response of ISO New England Inc.” *Response to Grid Resilience in Regional Transmission Organization and Independent System Operators* (AD18-7-000). March 9, 2018. [https://www.iso-ne.com/static-assets/documents/2018/03/ad18-7\\_iso\\_response\\_to\\_grid\\_resilience.pdf](https://www.iso-ne.com/static-assets/documents/2018/03/ad18-7_iso_response_to_grid_resilience.pdf).
- Jenkins, Brian Michael. “Countering al-Qaeda: The Next Phase in the War.” *The RAND Blog*, September 8, 2002. <https://www.rand.org/blog/2002/09/countering-al-qaeda-the-next-phase-in-the-war.html>.
- Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States*. Joint Publication 1. Washington, DC: Joint Chiefs of Staff, July 12, 2017. [http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1\\_ch1.pdf](http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf).
- Joint Commenters. “Comments of American Public Power Association, Large Public Power Council, National Rural Electric Cooperative Association, and Transmission Access Policy Study Group.” In *Response to RIN 1901-AB40*. February 23, 2017. <http://appanet.files.cms-plus.com/2-23-17%20DOE%20Comments%20RIN%201901-AB40.pdf>.
- Kaften, Cheryl. “DoD Tests Energy Continuity with ‘Islanded’ Microgrid.” *Energy Manager Today*, April 5, 2017. <https://www.energymanagertoday.com/dod-tests-energy-continuity-islanded-microgrid-0168957/>.
- Kappenman, John. *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*. Goleta, CA: Metatech, January 2010. [https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc\\_meta-r-319.pdf](https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf).
- “Key Players.” NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/AboutNERC/keyplayers/Pages/default.aspx>.
- Kissane, Carolyn, and Emily Medina. “Energy Aftershocks in Store after Seismic Mexican Election.” *The Hill*, July 3, 2018. <http://thehill.com/opinion/energy-environment/395383-energy-aftershocks-in-store-after-seismic-mexican-election>.



- Kramer, Franklin D., Robert J. Butler, and Catherine Lotrionte. *Cyber, Extended Deterrence, and NATO*. Washington, DC: Atlantic Council, May 2016. [http://www.atlanticcouncil.org/images/publications/Cyber\\_Extended\\_Deterrence\\_and\\_NATO\\_web\\_0526.pdf](http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf).
- Lawrence, Bill, Charlotte de Seibert, and Philip Daigle. "E-ISAC Update." Presentation at NERC's Critical Infrastructure Protection Committee Meeting, Jacksonville, FL, March 6–7, 2018. <https://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/March%202018%20CIPC%20Presentations.pdf>.
- Lazar, Jim. *Electricity Regulation in the US: A Guide*. 2nd ed. Montpelier, VT: Regulatory Assistance Project, June 2016. <http://www.raponline.org/wp-content/uploads/2016/07/rap-lazar-electricity-regulation-US-june-2016.pdf>.
- Lewis, James A. "North Korea and Cyber Catastrophe—Don't Hold Your Breath." *38 North*, January 12, 2018. <http://www.38north.org/2018/01/jalewis011218/>.
- . *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. Washington, DC: CSIS, January 2018. [http://espas.eu/orbis/sites/default/files/generated/document/en/180108\\_Lewis\\_ReconsideringCybersecurity\\_Web.pdf](http://espas.eu/orbis/sites/default/files/generated/document/en/180108_Lewis_ReconsideringCybersecurity_Web.pdf).
- Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–70. [http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06\\_Issue-3/Fall12.pdf](http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06_Issue-3/Fall12.pdf).
- Lucas, Todd. "Conservative Operations." Presentation at NERC's Monitoring & Situational Awareness Technical Conference, Denver, CO, September 18–19, 2013. <http://www.nerc.com/pa/rrm/Resources/MonitoringSituationalAwarenessDL/5.%20Event%20Response%20Strategies%20-%20SoCo%20-%20Todd%20Lucas.pdf>.
- Lynch, Justin. "How the Russian Government Allegedly Attacks the American Electric Grid." *Fifth Domain*, July 24, 2018. <https://www.fifthdomain.com/critical-infrastructure/2018/07/24/how-the-russian-government-attacks-the-american-electric-grid/>.
- Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (Sept./Oct. 2010). <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>.
- "Maritime Forces Pacific." Royal Canadian Navy. Last modified November 24, 2016. <http://www.navy-marine.forces.gc.ca/en/about/structure-marpac-home.page>.
- Marks, Joseph. "DHS Stands up New Cyber Risk Center to Protect High-Value Targets." *Nextgov*, July 31, 2018. <https://www.nextgov.com/cybersecurity/2018/07/dhs-stands-new-cyber-risk-center-protect-high-value-targets/150179/>.
- Marqusee, Jeffrey, Craig Schultz, and Dorothy Robyn. *Power Begins at Home: Assured Energy for U.S. Military Bases*. Reston, VA: Noblis, January 12, 2017. [http://www.pewtrusts.org/~media/assets/2017/01/ce\\_power\\_begins\\_at\\_home\\_assured\\_energy\\_for\\_us\\_military\\_bases.pdf](http://www.pewtrusts.org/~media/assets/2017/01/ce_power_begins_at_home_assured_energy_for_us_military_bases.pdf).
- McElwee, Steven. "Probabilistic Cluster Ensemble Evaluation for Unsupervised Intrusion Detection." Unpublished thesis, Nova Southeastern University, forthcoming.



- McElwee, Steven, Jeffrey Heaton, James Fraley, and James Cannady. "Deep Learning for Prioritizing and Responding to Intrusion Detection Alerts." In *2017 IEEE Military Communications Conference Proceedings*. Piscataway, NJ: IEEE, 2017. <https://ieeexplore.ieee.org/document/8170757/>.
- McGhee, Michael. "EEI Executive Advisory Committee." Slides presented at the EEI Annual Convention, Boston, MA, June 14, 2017. [http://www.asaie.army.mil/Public/ES/oei/docs/EEI\\_Exec-Committee.pdf](http://www.asaie.army.mil/Public/ES/oei/docs/EEI_Exec-Committee.pdf).
- Miller, James N. "Cyber Deterrence Cannot Be One Size Fits All." *Cipher Brief*, August 3, 2017. [https://www.thecipherbrief.com/column\\_article/cyber-deterrence-cannot-be-one-size-fits-all-1092](https://www.thecipherbrief.com/column_article/cyber-deterrence-cannot-be-one-size-fits-all-1092).
- Miller, James N., and James R. Gosler. "Memorandum for the Chairman, Defense Science Board" (preamble). In *Task Force on Cyber Deterrence*. Washington, DC: Defense Science Board, February 2017. <http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf>.
- Miller, James N., Jr., and Richard Fontaine. *A New Era in U.S.-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies Are Reshaping Pathways to Crisis and Conflict*. Washington, DC: CNAS, September 2017. <https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Project Pathways-Finalb.pdf?mtime=20170918101505>.
- Miller, Rich. "Con Edison Shuts off Power in Lower Manhattan." *DataCenter Knowledge*, October 29, 2012. <http://www.datacenterknowledge.com/archives/2012/10/29/con-edison-manhattan-power-shutdown>.
- MISO (Midcontinent Independent System Operator). *Geomagnetic Disturbance Operations Plan*. SO-P-AOP-01 Rev: 1. Carmel, IN: MISO, June 9, 2017. [https://old.misoenergy.org/\\_layouts/miso/ecm/redirect.aspx?id=252214](https://old.misoenergy.org/_layouts/miso/ecm/redirect.aspx?id=252214).
- . "MISO January 17–18 Maximum Generation Event Overview." Slides presented at the MISO Markets Subcommittee Meeting, Carmel, IN, February 8, 2018. <https://cdn.misoenergy.org/20180208%20MSC%20Item%2008%20Update%20on%20January%20Weather%20and%20Winter%20Storm%20Inga122372.pdf>.
- Mitchell, A. Weiss. "The Case for Deterrence by Denial." *American Interest*, August 12, 2015. <https://www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/>.
- "M-1 Reserve Margin." NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/pa/RAPA/ri/Pages/PlanningReserveMargin.aspx>.
- Murauskaite, Egle. "North Korea's Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment." *38 North*, September 12, 2014. <http://www.38north.org/2014/09/emurauskaite091214/>.
- Nakashima, Ellen. "U.S. Officials Say Russian Government Hackers Have Penetrated Energy and Nuclear Company Business Networks." *Washington Post*, July 8, 2017. [https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47\\_story.html](https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html).
- NARUC (National Association of Regulatory Utility Commissioners). *Cybersecurity: A Primer for State Utility Regulators*. Version 3.0. Washington, DC: NARUC, January 2017. <https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F>.

- . *Resolution on Physical Security*. Washington, DC: NARUC, July 16, 2014. <https://pubs.naruc.org/pub.cfm?id=53A0CAA5-2354-D714-5127-E0C411BAD460>.
- NASEO (National Association of State Energy Officials). “Comments of the National Association of State Energy Officials.” In *Response to RIN 1901–AB40*. [https://www.naseo.org/Data/Sites/1/naseo-comments\\_rin-1901%E2%80%93ab40.pdf](https://www.naseo.org/Data/Sites/1/naseo-comments_rin-1901%E2%80%93ab40.pdf).
- NATF (North American Transmission Forum). *Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—A Spare Tire Approach*. Charlotte, NC: NATF, 2017. <http://www.natf.net/docs/natf/documents/resources/natf-bes-operations-absent-ems-and-scada-capabilities---a-spare-tire-approach.pdf>.
- . *North American Transmission Forum External Newsletter*. Charlotte, NC: NATF, January 2018. <https://www.natf.net/docs/natf/documents/newsletters/natf-external-newsletter---january-2018.pdf>.
- National Defense Authorization Act for Fiscal Year 2017. Public Law 114-328. *U.S. Statutes at Large* 130 (2016): 2685–2687. <https://www.gpo.gov/fdsys/pkg/PLAW-114publ328/pdf/PLAW-114publ328.pdf>.
- NERC (North American Electric Reliability Corporation). *BAL-002-2(i)—Disturbance Control Standard—Contingency Reserve for Recovery from a Balancing Contingency Event*. Washington, DC: NERC, January 1, 2018. [https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2\(i\).pdf](https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-002-2(i).pdf).
- . *CIP-014-2—Physical Security*. Washington, DC: NERC, October 2, 2015. <http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf>.
- . *EOP-010-1—Geomagnetic Disturbance Operations*. Washington, DC: NERC, June 2014. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=EOP-010-1&title=Geomagnetic%20Disturbance%20Operations&jurisdiction=United%20States).
- . *EOP-011-1—Emergency Operations*. Washington, DC: NERC, April 1, 2017. [https://www.nerc.com/\\_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States](https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=EOP-011-1&title=Emergency%20Operations&jurisdiction=United%20States).
- . *Glossary of Terms Used in NERC Reliability Standards*. Washington, DC: NERC, last updated July 3, 2018. [https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary\\_of\\_Terms.pdf](https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf).
- . *Grid Security Exercise: GridEx III Report*. Atlanta, GA: NERC, March 2016. <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.
- . *Grid Security Exercise GridEx IV: Lessons Learned*. Atlanta, GA: NERC, March 28, 2018. <https://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20IV%20Public%20Lessons%20Learned%20Report.pdf>.
- . *History of NERC*. Washington, DC: NERC, August 2013. <http://www.nerc.com/AboutNERC/Documents/History%20AUG13.pdf>.
- . *Hurricane Harvey Event Analysis Report*. Washington, DC: NERC, March 2018. [https://www.nerc.com/pa/rrm/ea/Hurricane\\_Harvey\\_EAR\\_DL/NERC\\_Hurricane\\_Harvey\\_EAR\\_20180309.pdf](https://www.nerc.com/pa/rrm/ea/Hurricane_Harvey_EAR_DL/NERC_Hurricane_Harvey_EAR_20180309.pdf).

- . “Informational Filing on the Definition of ‘Adequate Level of Reliability.’” Filing to the Federal Energy Regulatory Commission. May 10, 2013. [https://www.nerc.com/pa/Stand/Resources/Documents/Adequate\\_Level\\_of\\_Reliability\\_Definition\\_\(Informational\\_Filing\).pdf](https://www.nerc.com/pa/Stand/Resources/Documents/Adequate_Level_of_Reliability_Definition_(Informational_Filing).pdf).
- . *IRO-008-2—Reliability Coordinator Operational Analysis and Real-Time Assessments*. Washington, DC: NERC, April 1, 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/IRO-008-2.pdf>.
- . *PRC-010-2—Under Voltage Load Shedding*. Washington, DC: NERC, April 2, 2017. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-010-2&title=Undervoltage%20Load%20Shedding&jurisdiction=United%20States).
- . *Reliability Guideline: Gas and Electrical Operational Coordination Considerations*. Atlanta, GA: NERC, December 13, 2017. [https://www.nerc.com/comm/OC\\_Reliability\\_Guidelines\\_DL/Gas\\_and\\_Electrical\\_Operational\\_Coordination\\_Considerations\\_20171213.pdf](https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Gas_and_Electrical_Operational_Coordination_Considerations_20171213.pdf).
- . *Reliability Terminology*. Atlanta, GA: NERC, August 2013. <https://www.nerc.com/AboutNERC/Documents/Terms%20AUG13.pdf>.
- . *Short-Term Special Assessment: Operational Risk Assessment with High Penetration of Natural Gas-Fired Generation*. Atlanta, GA: NERC, May 2016. [https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric\\_Final.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20Gas%20Electric_Final.pdf).
- . *Standard PRC-006-3—Automatic Underfrequency Load Shedding*. Washington, DC: NERC, October 1, 2017. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-006-3&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States).
- . *Technical Report Supporting Definition of Adequate Level of Reliability*. Washington, DC: NERC, March 26, 2013. <https://www.nerc.com/comm/Other/Pages/Adequate%20Level%20of%20Reliability%20Task%20Force%20ALRTF.aspx>.
- . *TOP-001-3—Transmission Operations*. Washington, DC: NERC, April 1, 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/TOP-001-3.pdf>.
- . *TPL-007-1—Transmission System Planned Performance for Geomagnetic Disturbance Events*. Washington, DC: NERC, December 2014. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States).
- . *2013 Special Reliability Assessment: Accommodating an Increased Dependence on Natural Gas for Electric Power Phase II: A Vulnerability and Scenario Assessment for the North American Bulk Power System*. Atlanta, GA: NERC, May 2013. [https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC\\_PhaseII\\_FINAL.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_PhaseII_FINAL.pdf).
- . *2016 Long-Term Reliability Assessment*. Atlanta, GA: NERC, December 2016. <https://www.nerc.com/pa/rapa/ra/reliability%20assessments%20dl/2016%20long-term%20reliability%20assessment.pdf>.
- . *VAR-001-4.2—Voltage and Reactive Control*. Washington, DC: NERC, September 2017. <https://www.nerc.com/pa/Stand/Reliability%20Standards/VAR-001-4.2.pdf>.

- NERC (North American Electric Reliability Corporation) Steering Group. *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* Princeton, NJ: NERC, July 13, 2014. [https://www.nerc.com/docs/docs/blackout/NERC\\_Final\\_Blackout\\_Report\\_07\\_13\\_04.pdf](https://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf).
- NERC (North American Electric Reliability Corporation) System Protection and Control Subcommittee. *Reliability Fundamentals of System Protection*. Princeton, NJ: NERC, December 2010. [https://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/Protection%20System%20Reliability%20Fundamentals\\_Approved\\_20101208.pdf](https://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/Protection%20System%20Reliability%20Fundamentals_Approved_20101208.pdf).
- NETL (National Energy Technology Laboratory). *Reliability, Resilience and the Oncoming Wave of Retiring Baseload Units—Volume I: The Critical Role of Thermal Units during Extreme Weather Events*. Washington, DC: DOE, March 13, 2018. <https://www.netl.doe.gov/research/energy-analysis/search-publications/vuedetails?id=2594>.
- Newman, Lily Hay. “Hacker Lexicon: What Is the Attribution Problem?” *Wired*, December 24, 2016. <https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/>.
- NIAC (National Infrastructure Advisory Council). *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*. Washington, DC: NIAC, August 2017. <https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf>.
- Nielsen, Kirstjen M. “National Cybersecurity Summit Keynote Speech.” DHS (Department of Homeland Security). Released July 31, 2018. <https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech>.
- “NOAA Space Weather Scales.” NOAA. April 2011. <https://www.swpc.noaa.gov/sites/default/files/images/NOAAscales.pdf>.
- “North America.” NERC (North American Electric Reliability Corporation). n.d. <https://www.nerc.com/AboutNERC/keyplayers/Pages/Canada.aspx>.
- “The North Atlantic Treaty.” North Atlantic Treaty Organization. April 4, 1949 (as amended). [https://www.nato.int/cps/ic/natohq/official\\_texts\\_17120.htm](https://www.nato.int/cps/ic/natohq/official_texts_17120.htm).
- Nye, Joseph S., Jr. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (Winter 2016/2017): 44–71. [https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC\\_a\\_00266](https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266).
- Obama, Barack. *Executive Order—Assignment of National Security and Emergency Preparedness Communications Functions*. Washington, DC: The White House, July 6, 2012. <https://obamawhitehouse.archives.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness->.
- . *Executive Order—Coordinating Efforts to Prepare the Nation for Space Weather Events*. Washington, DC: The White House, October 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/10/13/executive-order-coordinating-efforts-prepare-nation-space-weather-events>.
- . *Executive Order—Improving Critical Infrastructure Cybersecurity*. Executive Order 13636. Washington, DC: The White House, February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.



- . *Executive Order—National Defense Resources Preparedness*. Washington, DC: The White House, March 16, 2012. <https://obamawhitehouse.archives.gov/the-press-office/2012/03/16/executive-order-national-defense-resources-preparedness>.
- . *United States Cyber Incident Coordination*. Presidential Policy Directive 41. Washington, DC: The White House, July 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.
- ODNI (Office of the Director of National Intelligence). *A Common Threat Framework: A Foundation for Communication*. McLean, VA: ODNI, January 26, 2018.
- Orenstein, Daniel G., and Lexi C. White. *Emergency Declaration Authorities across All States and D.C.* Edina, MN: Network for Public Health Law, June 16, 2015. [https://www.networkforphl.org/\\_asset/gxrdwm/Emergency-Declaration-Authorities.pdf](https://www.networkforphl.org/_asset/gxrdwm/Emergency-Declaration-Authorities.pdf).
- Paradise, Theodore J., et al. “ISO-RTO Council Comments on Notice of Proposed Rulemaking Regarding Grid Security Emergency Orders: Procedures for Issuance—RIN 1901–AB40.” Email to Jeffrey Baumgartner, US Department of Energy, February 6, 2017. [http://www.isorto.org/Documents/Report/20170206\\_Final\\_IRC-DOE\\_NOPR\\_Comments\\_re\\_Grid\\_Security\\_Emergency.pdf](http://www.isorto.org/Documents/Report/20170206_Final_IRC-DOE_NOPR_Comments_re_Grid_Security_Emergency.pdf).
- Parfomak, Paul W. *Pipelines: Securing the Veins of the American Economy, Testimony before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Transportation Security*. Washington, DC: Congressional Research Service, April 19, 2016. <http://docs.house.gov/meetings/HM/HM07/20160419/104773/HHRG-114-HM07-Bio-ParfomakP-20160419.pdf>.
- Parfomak, Paul W., Richard J. Campbell, Robert Pirog, Michael Ratner, Phillip Brown, John Frittelli, and Marc Humphries. *Cross-Border Energy Trade in North America: Present and Potential*. Washington, DC: Congressional Research Service, January 30, 2017. <https://fas.org/sgp/crs/misc/R44747.pdf>.
- Perry, Richard (US secretary of energy). Letter to the Federal Energy Regulatory Commission. September 28, 2017. <https://energy.gov/sites/prod/files/2017/09/f37/Secretary%20Rick%20Perry%27s%20Letter%20to%20the%20Federal%20Energy%20Regulatory%20Commission.pdf>.
- Phillips, Tony. “Solar Shield—Protecting the North American Power Grid.” *NASA Science*, October 26, 2010. [https://science.nasa.gov/science-news/science-at-nasa/2010/26oct\\_solarshield](https://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield).
- PJM. “Comments and Responses of PJM Interconnection, L.L.C.” In *Response to Grid Resilience in Regional Transmission Organizations and Independent System Operators* (AD18-7-000). March 9, 2018. <http://pjm.com/-/media/documents/ferc/filings/2018/20180309-ad18-7-000.ashx>.
- . “Conservative Operations.” Training materials presented on January 27, 2015. <https://www.pjm.com/-/media/training/nerc-certifications/gen-exam-materials/gof/20160104-conservative-operations.ashx?la=en>.
- . *PJM Manual 13: Emergency Operations*. Rev. 65. Audubon, PA: PJM, January 1, 2018. <http://www.pjm.com/~/-/media/documents/manuals/m13.ashx>.



- Puryear, Cotton. "91st Cyber Brigade Activated as Army National Guard's First Cyber Brigade." *National Guard*, September 19, 2017. <http://www.nationalguard.mil/News/Article/1315685/91st-cyber-brigade-activated-as-army-national-guards-first-cyber-brigade/>.
- Reagan, Ronald. "The President's News Conference." August 12, 1986. Transcript. The American Presidency Project, Gerhard Peters and John T. Woolley. <http://www.presidency.ucsb.edu/ws/?pid=37733>.
- "Reliability Coordinators." NERC (North American Electric Reliability Corporation). As of June 1, 2015. <https://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx>.
- "REMEDYS: Research Exploring Malware in Energy Delivery Systems." Cyber Resilient Energy Delivery Consortium. March 26, 2018. <https://cred-c.org/researchactivity/remedys-research-exploring-malware-energy-delivery-systems>.
- "The Role of Microgrids in Helping to Advance the Nation's Energy System." DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/role-microgrids-helping>.
- "Roles and Responsibilities of Governments in Natural Resources." Natural Resources Canada. Last modified October 2, 2017. <http://www.nrcan.gc.ca/mining-materials/taxation/8882>.
- Rosenbach, Eric. "Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks." *Prepared Statement for the United States Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy*. June 12, 2017. [https://www.foreign.senate.gov/imo/media/doc/061317\\_Rosenbach\\_Testimony.pdf](https://www.foreign.senate.gov/imo/media/doc/061317_Rosenbach_Testimony.pdf).
- "Sandia's Grid Modernization Program Newsletter." Sandia National Laboratories. December 2017. <https://content.govdelivery.com/accounts/USDOESNLEC/bulletins/1c11ce6>.
- Schwartz, Ian. "Sen. Tillis: We Are Living in a Glass House Throwing Rocks Complaining about Election Interference." *RealClear Politics*, January 5, 2017. [https://www.realclearpolitics.com/video/2017/01/05/sen\\_tillis\\_we\\_are\\_living\\_in\\_a\\_glass\\_house\\_throwing\\_rocks\\_complaining\\_about\\_election\\_interference.html](https://www.realclearpolitics.com/video/2017/01/05/sen_tillis_we_are_living_in_a_glass_house_throwing_rocks_complaining_about_election_interference.html).
- "Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response." DOE (Department of Energy). February 14, 2018. <https://www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency>.
- SERC. *Conservative Operations Guidelines*. Guide-800-101. Charlotte, NC: SERC, May 20, 2015. [https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines\\_rev-0-\(05-20-15\).pdf?sfvrsn=2](https://www.serc1.org/docs/default-source/program-areas/standards-regional-criteria/guidelines/serc-conservative-operations-process-guidelines_rev-0-(05-20-15).pdf?sfvrsn=2).
- Severe Impact Resilience Task Force. *Severe Impact Resilience: Considerations and Recommendations*. Washington, DC: NERC, May 9, 2012. [https://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF\\_Final\\_May\\_9\\_2012-Board\\_Accepted.pdf](https://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF_Final_May_9_2012-Board_Accepted.pdf).

- Shelton, William L. "Threats to Space Assets and Implications for Homeland Security." *Written Testimony before the House Armed Services Subcommittee on Strategic Forces and House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications*. March 29, 2017. <http://docs.house.gov/meetings/AS/AS29/20170329/105785/HHRG-115-AS29-Wstate-SheltonW-20170329.pdf>.
- Sistrunk, Chris. "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)." *SANS Industrial Control Systems Security Blog*, January 8, 2016. <https://ics.sans.org/blog/2016/01/08/ics-cross-industry-learning-cyber-attacks-on-a-an-electric-transmission-and-distribution-part-one>.
- Slayton, Rebecca. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41, no. 3 (Winter 2016/17): 73–109. [https://www.mitpressjournals.org/doi/10.1162/ISEC\\_a\\_00267](https://www.mitpressjournals.org/doi/10.1162/ISEC_a_00267).
- Smith, Rebecca. "U.S. Officials Push New Penalties for Hackers of Electrical Grid." *Wall Street Journal*, August 5, 2018. <https://www.wsj.com/articles/u-s-officials-push-new-penalties-for-hackers-of-electrical-grid-1533492714>.
- Smith, Scott S. "Roles and Responsibilities for Defending the Nation from Cyber Attack." *Testimony Before the Senate Armed Services Committee*. October 19, 2017. <https://www.fbi.gov/news/testimony/cyber-roles-and-responsibilities>.
- Sobczak, Blake, Hannah Northey, and Peter Behr. "Cyber Raises Threat against America's Energy Backbone." *Energy Wire*, May 23, 2017. <https://www.eenews.net/stories/1060054924/>.
- Social Media Working Group for Emergency Services and Disaster Management. *Countering False Information on Social Media in Disasters and Emergencies*. Washington, DC: DHS, March 2018. [https://www.dhs.gov/sites/default/files/publications/SMWG\\_Countering-False-Info-Social-Media-Disasters-Emergencies\\_Mar2018-508.pdf](https://www.dhs.gov/sites/default/files/publications/SMWG_Countering-False-Info-Social-Media-Disasters-Emergencies_Mar2018-508.pdf).
- "Spare Transformers." EEI (Edison Electric Institute). n.d. <http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx>.
- Stanley, Andrew J. *Mapping the U.S.-Canada Energy Relationship*. Washington, DC: CSIS, May 2018. [https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180507\\_St Stanley\\_U.S.CanadaEnergy.pdf?fBwWhKl0BBuNMOeIRSolkNQ89Iij7iaz](https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180507_St Stanley_U.S.CanadaEnergy.pdf?fBwWhKl0BBuNMOeIRSolkNQ89Iij7iaz).
- "State and Local Energy Assurance Planning." DOE (US Department of Energy). n.d. <https://www.energy.gov/oe/services/energy-assurance/emergency-preparedness/state-and-local-energy-assurance-planning>.
- State of New Jersey Board of Public Utilities. *In the Matter of Utility Cyber Security Program Requirements* (Docket No. AO16030196). March 18, 2016. <http://www.nj.gov/bpu/pdf/boardorders/2016/20160318/3-18-16-6A.pdf>.
- Stockton, Paul. On behalf of Exelon Corporation. *Prepared Direct Testimony on Grid Reliability and Resilience Pricing*. Docket No. RM18-1-000. October 23, 2017.
- . "Thresholds and Criteria for Declaring Grid Security Emergencies." Study for the US Department of Energy. January 31, 2018.

- Sukumar, Arun M. "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?" *Lawfare* (blog), July 4, 2017. <https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.
- "Transmission Equipment Ready When Needed." Grid Assurance. n.d. <http://www.gridassurance.com/equipment-subscribers/>.
- Trump, Donald. *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Executive Order 13800. Washington, DC: The White House, May 11, 2017. <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.
- Ucci, Daniele, Leonardo Aniello, and Roberto Baldoni. "Survey on the Usage of Machine Learning Techniques for Malware Analysis." *ACM Transactions on the Web* 1, no. 1 (October 2017): 1:1–1:34. <https://pdfs.semanticscholar.org/d310/47e426b8b5c2aa52108899a800bedd966f07.pdf>.
- "United States Mandatory Standards Subject to Enforcement." NERC. n.d. <https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States>.
- U.S.-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Washington, DC: DOE, April 2004. <https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>.
- US Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Washington, DC: US Cyber Command, released March 2018. <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf>.
- Van Broekhoven, S. B., N. Judson, S. V. T. Nguyen, and W. D. Ross. *Microgrid Study: Energy Security for DoD Installations*. Technical Report 1164. Lexington, MA: MIT, June 2012. <https://www.ll.mit.edu/mission/engineering/Publications/TR-1164.pdf>.
- Vine, Doug. *Interconnected: Canadian and U.S. Electricity*. Arlington, VA: Center for Climate and Energy Solutions, March 2017. <https://www.c2es.org/site/assets/uploads/2017/05/canada-interconnected.pdf>.
- Walker, Bruce J. *Written Testimony before the U.S. Senate Committee on Energy and Natural Resources*. March 1, 2018. [https://www.energy.senate.gov/public/index.cfm/files/serve?File\\_id=1C574731-A9C0-4E1C-9E05-15C492E332B1](https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=1C574731-A9C0-4E1C-9E05-15C492E332B1).
- Weiss, Walter. "Rapid Attack Detection, Isolation and Characterization Systems (RADICS)." Defense Advanced Research Projects Agency. n.d. <https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems>.
- Western Electricity Coordinating Council. "Conservative System Operations." Training slides. n.d. <http://docplayer.net/55224883-Conservative-system-operations.html>.
- The White House. *National Security Strategy of the United States of America*. Washington, DC: The White House, December 2017. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
- "Work Continues on ITC Lake Erie Project." *Transmission Hub*, February 19, 2018. <https://www.transmissionhub.com/articles/2018/02/work-continues-on-itc-lake-erie-project.html>.



## Acknowledgments

My special thanks go to Robert Denaburg, senior analyst at Sonecon LLC. I also thank the following colleagues for helpful reviews of this study: Michael Assante (SANS Institute); Wayne Austad (Idaho National Laboratory); Terry Boston; Stuart Brindley; Gerry Cauley; Richard Danzig (JHU/APL); Daniel Elmore (Idaho National Laboratory); Peter Grandgeorge (Berkshire Hathaway Energy); Emily Goldman (US Cyber Command); Sean Griffin (ecubed us LLC); Dave Halla (JHU/APL); Jon Jipping (ITC Holdings); Debra Lavoy (Narrative Builders); Bill Lawrence (NERC); Joseph Maurio (JHU/APL); James Miller (JHU/APL); Michael Moskowitz (JHU/APL); Richard Mroz; Steven T. Naumann (Exelon Corporation); Catherine Peacock (JHU/APL); Emilia Probasco (JHU/APL); Erin Richardson (JHU/APL); David Roop (Dominion Energy); Matthew Schaffer (JHU/APL); senior leaders at Southern Company; Kyle Thomas (Dominion Virginia Power); and Virginia Wright (Idaho National Laboratory). I also thank the many additional industry and government reviewers who preferred to remain anonymous.

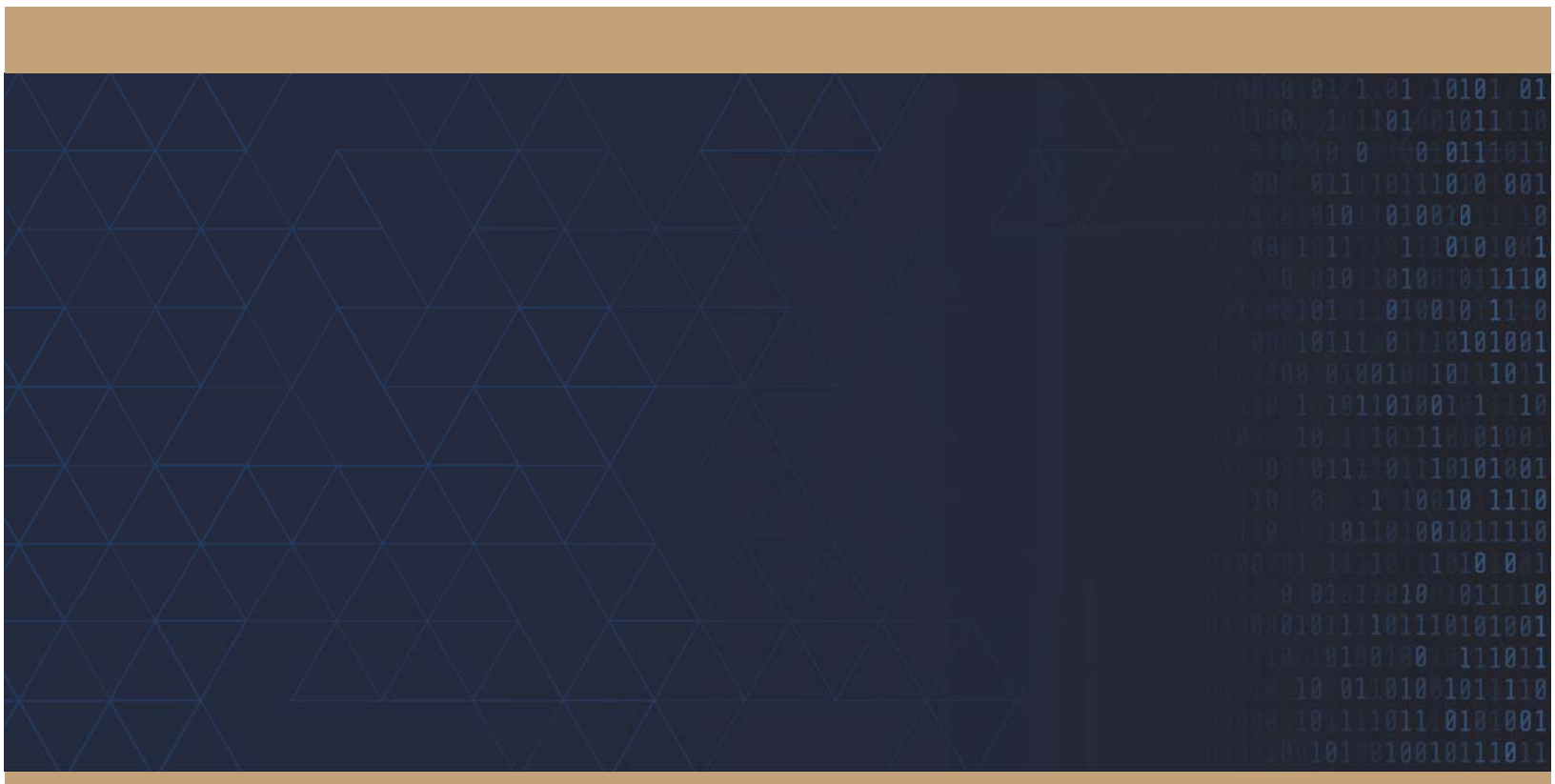
## About the Author

Paul Stockton is the managing director of Sonecon LLC, an economic and security advisory firm in Washington, DC, and a senior fellow of JHU/APL. Before joining Sonecon, he served as the assistant secretary of defense for Homeland Defense and Americas' Security Affairs from May 2009 until January 2013. In that position, he was the secretary of defense's principal civilian advisor on providing defense support in Superstorm Sandy and other disasters. Dr. Stockton also served as the Department of Defense (DOD) domestic crisis manager and was responsible for defense critical infrastructure protection policies and programs. In addition, Dr. Stockton served as the executive director of the Council of Governors and was responsible for developing and overseeing the implementation of DOD security policy in the Western Hemisphere. Prior to being confirmed as assistant secretary, Dr. Stockton served as a senior research scholar at Stanford University's Center for International Security and Cooperation, associate provost of the Naval Postgraduate School, and director of the school's Center for Homeland Defense and Security. Dr. Stockton was twice awarded the Department of Defense Medal for Distinguished Public Service, DOD's highest civilian award. DHS awarded Dr. Stockton its Distinguished Public Service Medal. Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He is the author of *Superstorm Sandy: Implications for Designing a Post-Cyber Attack Power Restoration System* (Laurel, MD: JHU/APL, 2016) and numerous other publications. He served as the facilitator of the GridEx IV exercise (November 2017) and is a member of the Homeland Security Advisory Council and other public and private sector boards.









From: [Andrew Dodge](#)  
To: (b) (6)  
Cc: (b) (5); [Andrew Dodge](#)  
Subject: OE and OER participation in visit from EU CEOs - ACTION REQUIRED  
Date: Friday, November 02, 2018 9:52:43 AM  
Attachments: [Energy Transition Forum Programme Washington DC 16102018.docx](#)  
[Participants List for Email - October 16.docx](#)

---

(b) (6)

Please add this to my calendar.

(b) (6)

Please work with your team to develop some slides and talking points for me. Please share a rough draft with me by Tuesday November 13<sup>th</sup>.

Please see the email below for more details. Let me know if you have any questions.

Thanks,

Andy

J. Andrew Dodge, Sr.  
Federal Energy Regulatory Commission  
Office of Electric Reliability (OER)  
888 First Street, 9M-01  
Washington, DC 20426  
Phone – 202-502-6101  
[Andrew.Dodge@ferc.gov](mailto:Andrew.Dodge@ferc.gov)

Note: This email and any files transmitted with it are the property of the sender and are intended solely for the use of the individual or entity to whom this email is addressed and should not be copied or forwarded to others without the permission of the sender. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender and delete this message immediately from your computer. Any other use, retention, dissemination, forward, printing, or copying of this message is strictly prohibited. Information contained herein is my opinion and view and not necessarily those of the United States Government, the Federal Energy Regulatory Commission, individual Commissioners, or other members of the Commission staff unless specifically stated.

---

**From:** Sandra Waldstein  
**Sent:** Thursday, November 01, 2018 2:30 PM  
**To:** Andrew Dodge <[Andrew.Dodge@ferc.gov](mailto:Andrew.Dodge@ferc.gov)>  
**Cc:** David Ortiz <[David.Ortiz@ferc.gov](mailto:David.Ortiz@ferc.gov)>  
**Subject:** FW: OE and OER participation in visit from EU CEOs

[Andrew](#),

Congratulations on your new position as Director of OER. I am organizing a meeting of a group of high level utilities and government officials who are coming to FERC on the afternoon of Wednesday, November 28<sup>th</sup>. David had kindly agreed to participate for OER.

John Jimison is the lead organizer for the Energy Transition Forum in partnership with the UN Foundation. John developed the agenda and asked for the participation of some of FERC's Office Directors. The session I'm asking you about is the one below which will share a 30 minute slot with OE. Would you like me to put you down as the speaker for OER?

I'm attaching the full agenda for this visit as well as a list of attendees. Please be advised that the FERC speakers are also invited to attend a reception and dinner that evening at the Hay-Adams hotel. FERC staff has been cleared for attendance at the evening events by GAL.

I will also send you a calendar invite. I would ask that each person attending do their best to stay for the full afternoon so they can engage in discussions with the participants.

Thanks,  
Sandie

***"FERC's Operations Center and Market Oversight Center"***

**Presenters:** *Larry Parkinson, Director, Office of Enforcement*

*David Ortiz, Director, Office of Electric Reliability*

FERC holds a unique position in the US regulatory landscape, supervising bulk power transmission rates and interstate natural gas sales, and the markets they affect. The Commission houses electronic Operations and Market Oversight Centers to enable it to perform its oversight effectively and rapidly. How does FERC use these centers to support system reliability and market stability?

*Sandra Waldstein*

*Director, Division of State, International & Public Affairs*

*Office of External Affairs*

*Federal Energy Regulatory Commission*

*202-502-8092*

*[sandra.waldstein@ferc.gov](mailto:sandra.waldstein@ferc.gov)*

---

**From:** Sandra Waldstein

**Sent:** Friday, July 20, 2018 12:26 PM

**To:** David Ortiz <[David.Ortiz@ferc.gov](mailto:David.Ortiz@ferc.gov)>; Larry Parkinson <[larry.parkinson@ferc.gov](mailto:larry.parkinson@ferc.gov)>

**Subject:** OE and OER participation in visit from EU CEOs

David, Larry,

We are hosting a group of utility CEOs in November, most of which are from Europe. They have asked for a summary of the work that we do both with the RMC (which they refer to as the 'Operations Center') and the MMC (or the 'Market Oversight Center')." They are devoting 45 minutes for this session and they are hoping to have FERC senior leaders come and talk to them about these activities. I believe Comm. Glick will be participating all day.

The date is Wednesday afternoon, November 28<sup>th</sup>. The time slot for this session is 3:00 – 3:45. We will be in the Commission Meeting Room as there could be up to 50 participants. We thought it best to have you both bring your presentation in to the CMR rather than try to take 50 people to the RMC and MMC. Perhaps you could use some slides with visuals of both rooms.

Could you please let me know if you would be able to participate? I'm trying to



identify speakers well in advance as they have asked for senior FERC leaders. I also expect that they would be amenable to any changes to the program description if you think that would be helpful.

In addition, you would both be invited to join the group for a reception and dinner later that evening.

.

Thanks,

Sandie

Here is a description of the session

3:00pm ***“FERC’s Operations Center and Market Oversight Center”***

**Speaker: Senior FERC staff, *[Need Names and Titles]***

FERC holds a unique position in the US regulatory landscape, supervising bulk power transmission rates and interstate natural gas sales, and the markets they affect. The Commission houses electronic Operations and Market Oversight Centers to enable it to perform its oversight effectively and rapidly. How does FERC use these centers to support system reliability and market stability?

3:30pm **Discussion with ETF Participants.**

*Sandra Waldstein*

*Director, Division of State, International & Public Affairs*

*Office of External Affairs*

*Federal Energy Regulatory Commission*

*202-502-8092*

*[sandra.waldstein@ferc.gov](mailto:sandra.waldstein@ferc.gov)*



## **Energy Transition Forum 3.0 Site Visit and Workshop 28-30 November 2018**

**Washington, DC, USA**

### ***“Emerging Threats and Opportunities: Cybersecurity, Political Change, and the Future of Natural Gas”***

The continuing transition in the energy industry faces new headwinds disruptions not just from technological change but from rapidly evolving cyber threats, sudden political shifts, and uncertainty about future role and sources of natural gas.

At the next session of the Energy Transition Forum in Washington, D.C., we will discuss these issues with experts from the US Federal Energy Regulatory Commission, political insiders and global industry experts.

#### **Themes:**

- *Implications of the U.S. mid-term elections for energy and climate policy*
- *Key driver in the electricity and gas sector: regulation or market forces*
- *The energy transition on the ground: latest developments and implications*
- *Cybersecurity challenges and responses by power companies and authorities*
- *The evolving role of natural gas in the energy transition*

***Organized by the Energy Transition Forum  
in partnership with the United Nations Foundation***



*We thank the Sponsors of the Energy Transition Forum:*



### Background Information – The Energy Transition Forum 3.0

The Energy Transition Forum (ETF) seeks to generate frank discussion, innovative thinking, and concrete solutions and actions around the ways in which participants from the United States, Europe and Asia can work together to achieve a timely and responsible transition to a secure, affordable and low-carbon global energy system, with emphasis on the rapidly evolving electric power industry.

The ETF does this through a series of facilitated off-the-record dialogues between influential energy leaders (C-level) from the private and public sectors, academic thought leaders and subject-matter experts that look at the impact of the latest energy challenges, new market entrants and energy technologies to define potential solutions in terms of innovative market and financial mechanisms, new business models and reforms to policy and regulation.

Initiated in 2012 by the transatlantic think tank “The German Marshall Fund of the United States”, the Energy Transition Forum has been successfully working ever since to address the increasingly complex challenges of the energy value chain, based on the implementation of the two ETF pillars: **“total systems thinking”** and the **“dialogue method”**.

This approach has already catalyzed surprising business and political insights, cutting-edge thinking, and practical innovative solutions. Perhaps even more importantly, the ETF’s structure has led to strong personal commitments, effective relationships and a “coalition of people” who are strongly motivated to understand, navigate and accelerate the on-going energy transition within their own professional environment, producing a “pebble in the pond” effect.

**“Never doubt that a small group of thoughtful, committed citizens  
can change the world. Indeed, it’s the only thing that ever has.”**

**– Margaret Mead, Cultural Anthropologist**

When the first incubation period of the ETF at the German Marshall Fund came to a natural end, participants urged that the program continue. Thus was launched “ETF 2.0” in October 2015. Two years later, a similar reassessment led to a new program of activity (“ETF 3.0”) with workshops in Berlin and Washington, D.C., in 2018. Future workshops are envisioned for Europe and potentially Asia in 2019.

The ETF is chaired by Miriam Maes in London, with support in Europe from Christophe Brognaux and Gerard Reid and in the US from Reid Detchon, John Jimison, Andy Ott and Jon Wellinghoff. The ETF’s sponsors, whose contributions make the ETF possible, include Boston Consulting Group, California ISO, Citigroup, EirGrid, IBM, Innowatts, National Grid, Siemens, Smart Wires, and UK Power Networks.



**Washington, DC – 28-30 November 2018**

***“Emerging Threats and Opportunities:  
Cybersecurity, Political Change, and the Future of Natural Gas”***

*A highly interactive discussion and deeper dialogue is at the core of every Energy Transition Forum workshop. Each participant serves as a “speaker” throughout the two days by contributing their perspectives, based on their own experiences and observations, and sharing their questions and uncertainties. The high level and broad range of participants – representing the different industries along the value chain, as well as governments and academia – combined with the intimacy of the group and use of the Chatham House Rule, ensures a lively, candid, and productive exchange of views. Selected participants are asked to prepare comments in advance of the workshop, to “seed” each discussion.*

**Wednesday, November 28<sup>th</sup>**

10:15am Transport from Hay Adams Hotel to Capitol Hill  
Hay-Adams Hotel  
800 16<sup>th</sup> Street, NW  
Washington, DC 20006

11:00am **Briefing on Capitol Hill**  
Capitol Visitor Center  
East Capitol Street and First Street, NE  
Washington, DC 20002

**Session Objectives**

- 1) Understand the implications of the US mid-term elections on energy and environmental policy as perceived by leaders of the US Congress
- 2) Discuss impacts of policy on practical challenges faced by utilities globally, especially cybersecurity, new market entrants, and the future of natural gas.

***“The Outlook for Energy Legislation in 2019-20”***

Panel discussion with senior policy staff from Republican and Democratic offices



- 12:15pm Luncheon and discussion with Congressional energy leaders (Venue TBD)  
***“Bringing Climate Change Imperatives Back into US Energy Policy”***  
**Presenters:**  
***US Representatives Carlos Curbelo (R., Florida) and Peter Welch (D., Vermont)*** (Invited)  
*Chair and Member, respectively, of the Congressional Climate Solutions Caucus*
- 1:45pm **Travel to Federal Energy Regulatory Commission (FERC)**  
*FERC Hearing Room  
 888 First Street, NE  
 Washington DC 20426*
- Session Objectives**

  - 1) Understand the roles of federal versus state and local utility regulation in the US, particularly in contrast to regulators in Europe and the rest of the world
  - 2) Learn the US federal government’s approach towards dealing with cybersecurity and physical threats to the grid, both now and as planned
  - 3) Discuss FERC’s role in the US power markets, including the novel market mechanisms developed for energy efficiency and demand response
  - 4) Hear the perspective of the key staff on how the grid is evolving and what FERC’s role needs to be in shaping that evolution.
- 2:00pm Arrival at FERC for passport and security check  
***Please bring your passport or other formal identity papers!***  
*(Luggage can be left securely in a room near the entrance to the building)*
- 2:15pm **Welcome and Introduction to FERC**  
**Speakers: *Sandra Waldstein*, Director, Division of State, International and Public Affairs**  
***David Morenoff*, Deputy General Counsel**  
 The Federal Energy Regulatory Commission is an independent US agency. Its five members are nominated by the President and approved by the Senate. FERC has the obligation to ensure that the wholesale power markets and transmission grid operate with reasonable rates, without undue discrimination, and with reliability and resilience. Direct regulation of utilities is the responsibility of the States.
- 2:30pm ***“The Resilience of the Grid: Cybersecurity, Physical Security and the Energy Transition”***  
**Speaker: *Joseph McClelland*, Director, Office of Energy Infrastructure Security**  
 As generation becomes more decentralized and integrated with transmission and distribution through digital technologies, the risks of cyber-attacks are increasing. As shown by the 2013 attack on the PG&E Metcalf substation in the US, physical security cannot be ignored. What is being done at the federal level to protect against these threats?
- 2:45pm **Discussion with ETF participants**

3:00pm **Moderator: John Jimison, Executive Director, Americans for a Clean Energy Grid, USA**  
**“FERC’s Operations Center and Market Oversight Center”**

**Presenters:** **Larry Parkinson, Director, Office of Enforcement**  
**David Ortiz, Director, Office of Electric Reliability**

FERC holds a unique position in the US regulatory landscape, supervising bulk power transmission rates and interstate natural gas sales, and the markets they affect. The Commission houses electronic Operations and Market Oversight Centers to enable it to perform its oversight effectively and rapidly. How does FERC use these centers to support system reliability and market stability?

3:30pm **Discussion with ETF participants**

3:45pm Tea and coffee break

4:15pm **“Challenges of the Transition from a US Federal Regulatory Perspective**

As the transition in the electric sector changes the technologies, the competitive landscape, the utility business models, the roles and options of customers, and the environmental, reliability, and resilience challenges of the sector, how do the heads of FERC’s key offices see the Commission’s evolving regulatory and market-supervising roles? What challenges do they see ahead for the Commission? Are 20<sup>th</sup>-century laws and regulatory jurisdictions impeding the transition to a 21<sup>st</sup>-century power grid?

**Presenters:** **Jignasa Gadani, Acting Head, Office of Energy Policy and Innovation**  
**Richard O’Neill, Chief Economic Advisor**  
**Anna Cochrane, Head, Office of Energy Market Regulation**

5:00pm **Discussion with ETF participants**

**Moderator: John Jimison, Executive Director, Americans for a Clean Energy Grid, USA**

6:00pm Transport to Hay-Adams Hotel  
 800 16<sup>th</sup> Street, NW  
 Washington, DC 20006

6:30pm **Reception sponsored by PJM Interconnection**

7:30pm **Dinner sponsored by Siemens, inviting FERC Commissioners and Senior Staff**  
*The Metropolitan Club, Grill Room*  
 1700 H St NW  
 Washington, DC 20006

**Please note: Business attire is required by the Club (coat and tie for men)**

**Welcome: Armin Schnettler, Head of Research in Energy and Electronics, Siemens**  
*Corporate Technology*



**Remarks: “The Key Challenges of the Energy Transition from the Perspective of the Climate Targets and the Realistic Pathways to Achieve Them”**

**Speaker: *Rachel Kyte*, Chief Executive Officer of Sustainable Energy for All, and Special Representative of United Nations Secretary-General António Guterres for Sustainable Energy for All**

Ms. Kyte served until December 2015 as World Bank Group Vice President and Special Envoy for Climate Change, leading the Bank Group’s efforts to campaign for an ambitious agreement at the 21st Convention of the Parties of the UNFCCC (COP 21). She was previously World Bank Vice President for Sustainable Development and was the International Finance Corporation Vice President for Business Advisory Services. Recipient of numerous awards for women’s leadership, climate action and sustainable development, she is a Professor of practice in sustainable development at the Fletcher School of Law and Diplomacy at Tufts University. She holds a master’s degree in international relations from Fletcher, and a bachelor’s degree in history and politics from the University of London.

**Keynote Remarks: “Looking at the Transition in the Energy Sector from the Perspective of the US Senate”**

**Speaker TBD**

## **Thursday, November 29<sup>th</sup>**

- 8:30am **Continental breakfast and networking**  
*United Nations Foundation  
 Board Room, 12<sup>th</sup> Floor  
 1750 Pennsylvania Avenue, NW  
 Washington, D.C. 20006*
- 9:00am **Welcome: *Pete Ogden*, Vice President for Energy, Climate and the Environment, United Nations Foundation**
- 9:15am **Introduction to the Energy Transition Forum**  
*Miriam Maes, Co-Chair, Energy Transition Forum, UK; Chairman, Supervisory Board, Port of Rotterdam, Netherlands*
- 9:45am **“Check-in” and self-introduction of participants**  
*Reid Detchon, Senior Advisor for Climate Solutions, United Nations Foundation*
- 10:45am Tea and coffee break
- 11:00am **Session 1: Implications of the US mid-term elections**

The 2018 mid-term elections in November 2018 offer the potential of change in the control of the US Congress and the power of the White House. This panel of political experts will discuss what the electoral results mean for the political direction of the United States, including energy and environment policy, and for US participation in the global energy transition and movement toward a decarbonized economy.

#### **Session Objectives**

- 1) Learn what messages voters sent to Washington in the mid-term elections and the impacts on the strategy and prospects for re-election of President Trump in 2020.
- 2) Understand the implications of the US election for energy and environmental policy in the Congress, the Trump administration, and US foreign policy.

**Moderator:** *Reid Detchon*

**Presenter:** *Geoffrey Garin, President, Hart Research, a company at the cutting edge of strategic and public opinion research*

**Discussants:** *John Podesta, former White House Chief of Staff and Counselor, Presidents Obama and Clinton; Founder, Center for American Progress*  
*Jerry Taylor, President, Niskanen Center, a non-partisan think tank*  
*Vic Fazio, former Congressman; Senior Advisor, Akin Gump*

12:15pm

Break for lunch and personal time



#### **12:45 pm “The Role of Federal Regulators as the Energy Transition Continues”**

**Speaker:** *Richard Glick, Commissioner, Federal Energy Regulatory Commission*

Commissioner Richard Glick has served since November 2, 2017. Before joining the Commission, Commissioner Glick was general counsel for the Democrats on the Senate Energy and Natural Resources Committee. Commissioner Glick was vice president of government affairs for Iberdrola’s renewable energy, electric and gas utility, and natural gas storage businesses in the United States, and previously served as a director of government affairs for PPM Energy and director of government affairs for PacifiCorp. He served as a senior policy advisor to U.S. Energy Secretary Bill Richardson, and before that was legislative director and chief counsel to U.S. Senator Dale Bumpers of Arkansas.

1:15pm

### **Session 2: The transition on the ground: latest developments and implications**

#### **Session Objectives**

- 1) Understand the challenges and opportunities created by the transition in the US
- 2) Discuss the influence of the regulatory compact – and the pros and cons of light-handed government oversight and the freedom to innovate vs. strong regulatory intervention
- 3) Understand how evolutions and challenges are different by market and whether strategies employed in another global market might also be relevant in your own.

**“What’s happening, what is working well, what do we need to fix?”**

**Moderator:** *Tom Baker, Partner and Managing Director, The Boston Consulting Group, USA*

**Panel:** *Pat Hogan, Senior Vice President of Electric Operations, Pacific Gas and Electric Company, USA*

*Stephen Prince, CEO, Centrica Business Solutions North America, Centrica, USA*

*Kathleen Barrón, Senior Vice President, Government and Regulatory Affairs and Public Policy, Exelon Corporation; Former Deputy General Counsel, FERC, USA*

Group discussion: Pros and cons of light-handed vs. strong electric sector regulation

2:30pm

**“How the transition differs around the world and how it doesn’t”**

Brief comments on three regions:

**Europe:** *Suleman Alli, Director, Strategy & Regulation, UK Power Networks, UK*

**China:** *Felix Zhang, Group Executive Director and Venture Partner, Envision Energy (renewable energy), China/USA*

**India:** *Rajiv Mishra, Managing Director India, China Light and Power, India*

Questions and comments from the full audience

3:00pm

Tea and coffee break

3:15pm

**Session 3: Cybersecurity: what is at stake and how to address it**

Cybersecurity concerns have recently taken center stage in a context of increasing digitalization of the economy and geopolitical tensions. In the case of power systems, cyber threats have since long been a preoccupation of operators. Transition to smart grids, decentralized energy generation, and proliferation of connected devices have led to exponential increases in cyber-attacks on the grid, some of them successful.

**Session Objectives**

- 1) Confirm the current understanding of resilience and cybersecurity risks in the energy system, in a context of increasingly decentralized energy
- 2) Discuss appropriate responses – managerially, technically, and in term of regulation and policy – to mitigate these risks and remedy them, whether at state, national or international level
- 3) Learn how your cyber-protection strategies compare with those of other utilities around the globe.

**Moderator:** *Gerard Reid, Co-Founder & Partner, Alexa Capital, UK*

**Introduction and short demonstration (by video conference)**

*Mohamed Harrou, Senior Engineer, Supervisory Control and Data Acquisition, BayWA (German trading house with large renewable development and virtual power plant business)*

3:45pm

**Opening remarks:** *Karen Evans (Invited), Assistant Secretary for the Office of Cybersecurity, Energy Security, and Emergency Response*



4:00pm

**Cybersecurity and the Energy Transition: a problem statement:**

How secure is the practical resilience and how high are the cyber security risks in our energy system? Do the risks of resilience and cyber increase or decrease in the context of increasingly decentralized energy?

**Panel:** ***Fintan Slye**, CEO, UK System Operator, National Grid, UK; former CEO, EirGrid, Ireland*

***Stephen Callahan**, Vice President of Global Strategy and Solutions for the Energy & Utilities Industry, IBM*

***Theresa Payton**, President and CEO, Fortalice Solutions; CIO, President George W. Bush Administration, USA*

4:45pm

**Addressing cybersecurity**

1. What should be the appropriate responses – managerially, technically, and in term of regulation and policy – to mitigate these risks and remedy them, whether at state, national or international level?
2. How do the cyber-protection strategies compare with those of other utilities around the globe?

**Panel:** ***Michael Coden**, Managing Director, Head of Cybersecurity Practice*

***Nadya Bartol**, Associate Director, BCG Platinion, USA*

***Harald Schrimpf**, CEO, PSI Software AG, Germany*

In their interventions, Michael/Nadya and Harald will demonstrate how cybersecurity can become business-enabling within a utility. This can be done by creating converged governance, implementing robust cyber portfolio management, proactively addressing regulatory compliance, investing into talent acquisition and appropriate technologies, and changing the culture to view cybersecurity similarly to safety.

5:30pm

Questions, comments, and discussion with the whole audience

6:15pm

Closing remarks and break for group photo

6:30pm

Walk to Hay-Adams Hotel

7:00pm

**Reception and Dinner sponsored by PJM Interconnection**

*Hay-Adams Hotel Terrace (Top Floor)  
800 16<sup>th</sup> Street, NW  
Washington, DC 20006*

**Welcome:** ***Andy Ott**, CEO, PJM Interconnection and Co-Chair Energy Transition Forum*



**Keynote Remarks: “Perspectives on the Energy Transition in the US and Globally”**

**Speaker: Ernest J. Moniz**, *former US Secretary of Energy; Professor of Physics, MIT; President & CEO, Energy Futures Initiative*

Ernie Moniz is a nuclear physicist who served under President Obama as Secretary of Energy from 2013 to 2017. His accomplishments include leading an international initiative that placed energy science and technology innovation at the center of the global response to climate change and negotiating the historic Iran nuclear agreement alongside Secretary of State John Kerry. At MIT, Dr. Moniz was the Founding Director of the MIT Energy Initiative (MITEI) and Director of the Laboratory for Energy and the Environment. He received a Bachelor of Science degree summa cum laude in physics from Boston College and a doctorate in theoretical physics from Stanford University.

### Day 3: Friday, November 30<sup>th</sup>

8:30am **Continental breakfast and networking**

*United Nations Foundation  
Board Room, 12<sup>th</sup> Floor  
1750 Pennsylvania Avenue, NW  
Washington, D.C. 20006*

9:00am **Welcome back and “check-in”**  
**Moderator: Reid Detchon**

9:30am **Session 4: The Future Role of Natural Gas**

**Moderator: John Jimison**

While the energy transition has put coal and oil under pressure globally, gas has gained momentum due to abundance from shale production and relatively stable pricing. In the US, this has caused a shift in power generation from coal to gas. It has also impacted global gas markets, creating a de facto cap on prices and limiting the risk of high gas prices. With shale gas discoveries in other parts of the world such as Argentina, China and Australia, will natural gas will become the fuel of choice for the energy transition?

Gas is preferable to coal or petroleum in terms of carbon emissions and other pollutants – yet far from carbon-free: Questions remain about reducing methane leakage and whether the CO<sub>2</sub> production from gas combustion – half that of coal – is tolerable if we are to avoid catastrophic climate change. And gas may rapidly become economically vulnerable to zero-emission, zero-marginal-cost renewables. Will the perspective of further regulatory restrictions on emissions, combined with the ever-decreasing cost of renewables and other technologies, limit gas in many regions to a short-term “bridge” role?

#### **Session Objectives**

- 1) Understand the impact of the natural gas boom in North America on US and global energy policy and learn the decline rates of hydro fractured gas-well production.
- 2) Discuss whether natural gas is a "transition fuel" or a long-term solution in the context of the energy transition, and what this means for future investments in new gas generation, including risks of stranded assets.

#### **The geopolitics of natural gas**

**Melanie Kenderdine**, Principal, Energy Futures Initiative; former Director, Energy Policy and Systems Analysis, Counselor to Secretary Moniz, Department of Energy, USA

#### **Dynamics and challenges in natural gas markets**

**Christophe Brognaux**, Senior Partner and Managing Director, The Boston Consulting Group, Belgium

Questions, comments and discussion from the audience

#### **How much should we count on gas to achieve the energy transition?**

**Mark Brownstein**, Senior Vice President for Energy, Environmental Defense Fund  
**Chad Holliday**, Chairman of the Board, Royal Dutch Shell, Netherlands  
 [To be confirmed], Total, France  
**Don Santa**, President, Interstate Natural Gas Association; former Commissioner, FERC; former Senior Staff, Senate Energy Committee, USA

11:30am Summary of key takeaways from the workshop

**Tom Baker**, Partner, Boston Consulting Group

12:00pm “Check-out” and feedback from participants; suggestions of key topics for future ETFs

12:30pm Informal lunch and closure

=====



## Confirmed Participants Energy Transition Forum, 28-30 November 2018, Washington, DC

### US Utilities

- **Kathleen Barrón**, Senior Vice President, Competitive Market Policy, Exelon; former Deputy General Counsel, FERC, USA
- **John DiStasio**, President, Large Public Power Council, USA
- **Pat Hogan**, Senior Vice President of Electric Operations, Pacific Gas and Electric Company, USA
- **Phil Moeller**, Executive Vice President, Business Operations Group and Regulatory Affairs, Edison Electric Institute; former Commissioner, Federal Energy Regulatory Commission, USA
- **Andy Ott**, President and CEO, PJM Interconnection, USA
- **Stephen Prince**, CEO, Centrica Business Solutions North America, USA
- **Eric Schmitt**, VP of Operations, California Independent System Operator, USA
- **Gordon van Welie**, President and CEO, New England Independent System Operator, USA
- **Rudy Wynter**, President & COO - Transmission, Generation and Energy Procurement National Grid US, USA

### Utilities, Other Regions

- **Suleman Alli**, Director, Strategy & Regulation, UK Power Networks, UK
- **Bente Hagem**, Board Chair, ENTSO-E (European Network of Transmission System Operators); Executive Vice President for European Affairs, Statnett, Norway
- **Rajiv Mishra**, Managing Director India, China Light and Power, India
- **Derek Parkin**, Chief Operating Officer, China Light and Power, Hong Kong
- **Fintan Slye**, CEO, UK System Operator, National Grid, UK; former CEO, EirGrid, Ireland

### IT, Technology and New Energy Companies

- **Stephen Callahan**, Vice President of Global Strategy and Solutions for the Energy & Utilities Industry, IBM, USA
- **Gregg Rotenberg**, CEO, Smart Wires (transmission management solutions), USA
- **Harald Schrimpf**, Chairman, PSI Software (software solutions for utilities and industry incl. energy management systems), Germany
- **Michael Walsh**, Managing Director Europe, Smart Wires, (transmission management solutions), UK
- **Felix Zhang**, Group Executive Director and Venture Partner, Envision Energy (renewable energy), China/USA

### **Other Industry, Finance and Professional Services**

- **Tom Baker**, Partner and Managing Director, Global Topic Leader, Distributed Energy Resources, Boston Consulting Group, USA
- **Chad Holliday**, Chairman of the Board, Royal Dutch Shell, Netherlands
- **John Lynch**, Managing Director for Principal Investments, J.P. Morgan Asset Management - Infrastructure Investments Group, UK
- **Armin Schnettler**, Senior VP, Research in Energy and Electronics, Siemens, Germany
- **Sam Shakir**, CEO, Orano USA, USA

### **Government Authorities**

- **Jens Acker**, Counselor, Energy Trade, Digital Economy, Embassy of the Federal Republic of Germany, Germany
- **Dominique Jamme**, Advisor to the President, French Regulatory Commission "CRE", France
- **Richard Kauffman**, Chairman of Energy Policy and Finance, Office of the Governor, State of New York, USA
- **Melanie Kenderdine**, Principal, Energy Futures Initiative; former Director, Energy Policy and Systems Analysis and Energy Counselor to Secretary Moniz, Department of Energy, USA
- **Gerassimos Thomas**, Deputy Director General for Energy, European Commission, Belgium
- **Jon Wellinghoff**, CEO, GridPolicy Consulting; former Chairman, FERC, USA

### **NGOs**

- **Mark Brownstein**, Senior Vice President of Energy, Environmental Defense Fund, USA
- **Matt Futch**, Global Strategy and Business Development Director, NREL, USA
- **Mike Howard**, President and CEO, Electric Power Research Institute, USA
- **Peter Ogden**, Vice President, United Nations Foundation, USA
- **Rich Powell**, Executive Director, ClearPath Energy Action, USA
- **Barbara Tyran**, Executive Director, Government & External Relations, Electric Power Research Institute, USA

### **Speakers at FERC**

- **Anna Cochrane**, Director Office of Market Regulation, FERC, USA
- **Jignasa Gadani**, Acting Director Office of Energy Policy and Innovation, FERC, USA
- **Joe McClelland**, Director Office of Energy Infrastructure Security, FERC, USA
- **David Ortiz**, Acting Director Office of Electric Reliability, FERC, USA
- **Larry Parkinson**, Director Office of Enforcement, FERC, USA



### **Speakers at the Energy Transition Forum**

- **Nadya Bartol**, Associate Director, BCG Platinion, USA
- **Michael Coden**, Managing Director, Head of Cybersecurity Practice, BCG Platinion, USA
- **Vic Fazio**, Senior Advisor, Akin Gump; Former Congressman (CA), US Congress
- **Geoffrey Garin**, President, Hart Research, USA
- **Richard Glick**, Commissioner, FERC, USA
- **Rachel Kyte**, Chief Executive Officer, Sustainable Energy for All; Special Representative of the United Nations Secretary-General António Guterres, United Nations, USA
- **Ernest Moniz**, former US Secretary of Energy; Professor of Physics, MIT; President & CEO, Energy Futures Initiative
- **Theresa Payton**, President and CEO, Fortalice Solutions; CIO, President George W. Bush Administration, USA
- **John Podesta**, Founding President, Center for American Progress; Former White House Chief of Staff and Counsellor, Presidents Obama and Clinton, USA
- **Don Santa**, President, Interstate Natural Gas Association; former Commissioner, FERC; former Senior Staff, Senate Energy Committee, USA
- **Jerry Taylor**, President, The Niskanen Center, USA

### **Energy Transition Forum Team**

- **Miriam Maes**, Chair, Energy Transition Forum; Chairman, Supervisory Board, Port of Rotterdam, UK
- **Christophe Brognaux**, Senior Partner and Managing Director, The Boston Consulting Group, Belgium
- **Reid Detchon**, Senior Advisor for Climate Solutions, United Nations Foundation, USA
- **John Jimison**, Executive Director, Americans for a Clean Energy Grid, USA
- **Gerard Reid**, Co-Founder & Partner, Alexa Capital, UK
- **Kevin Head**, Programme Associate, Energy Transition Forum, UK/USA

**From:** (b) (6)  
**To:** (b) (6)  
**Cc:** (b) (6)  
**Subject:** RE: Item to add to the reference list  
**Date:** Thursday, September 20, 2018 9:56:04 AM  
**Attachments:** [Enhancing the Resilience of the Nation's Electricity System.pdf](#)

---

(b) (6)

Here is a copy, I placed the PDF in our folder for the data gathering effort.

(b) (6)

Office of Energy Infrastructure Security (OEIS)  
Federal Energy Regulatory Commission  
888 First Street, NE, Suite 91-59  
Washington, DC 20426

(b) (6)

---

**From:** (b) (6)

**Sent:** Thursday, September 20, 2018 9:14 AM

**To:** (b) (6)

**Subject:** Item to add to the reference list

<https://www.nap.edu/catalog/24836/enhancing-the-resilience-of-the-nations-electricity-system>

This PDF is available at <http://nap.edu/24836>

SHARE



## Enhancing the Resilience of the Nation's Electricity System

### DETAILS

170 pages | 8.5 x 11 | PAPERBACK

ISBN 978-0-309-46307-2 | DOI 10.17226/24836

### CONTRIBUTORS

Committee on Enhancing the Resilience of the Nation's Electric Power Transmission and Distribution System; Board on Energy and Environmental Systems; Division on Engineering and Physical Sciences; National Academies of Sciences, Engineering, and Medicine

GET THIS BOOK

FIND RELATED TITLES

Visit the National Academies Press at [NAP.edu](http://NAP.edu) and login or register to get:

- Access to free PDF downloads of thousands of scientific reports
- 10% off the price of print titles
- Email or social media notifications of new titles related to your interests
- Special offers and discounts



Distribution, posting, or copying of this PDF is strictly prohibited without written permission of the National Academies Press. ([Request Permission](#)) Unless otherwise indicated, all materials in this PDF are copyrighted by the National Academy of Sciences.

Copyright © National Academy of Sciences. All rights reserved.

# Enhancing the **RESILIENCE** of the Nation's Electricity System

Committee on Enhancing the Resilience of the  
Nation's Electric Power Transmission and Distribution System

Board on Energy and Environmental Systems

Division on Engineering and Physical Sciences

A Consensus Study Report of  
*The National Academies of*  
SCIENCES • ENGINEERING • MEDICINE

THE NATIONAL ACADEMIES PRESS

*Washington, DC*

[www.nap.edu](http://www.nap.edu)

**THE NATIONAL ACADEMIES PRESS**

**500 Fifth Street, NW**

**Washington, DC 20001**

This activity was supported by Grant No. EE-0007045 from the U.S. Department of Energy. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of any organization or agency that provided support for the project.

International Standard Book Number 13: 978-0-309-46307-2

International Standard Book Number 10: 0-309-46307-6

Library of Congress Control Number: 2017953067

Digital Object Identifier: <https://doi.org/10.17226/24836>

Additional copies of this publication are available for sale from the National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20001; (800) 624-6242 or (202) 334-3313; <http://www.nap.edu>.

Copyright 2017 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

Suggested citation: National Academies of Sciences, Engineering, and Medicine. 2017. *Enhancing the Resilience of the Nation's Electricity System*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/24836>.



*The National Academies of*  
**SCIENCES • ENGINEERING • MEDICINE**

The **National Academy of Sciences** was established in 1863 by an Act of Congress, signed by President Lincoln, as a private, nongovernmental institution to advise the nation on issues related to science and technology. Members are elected by their peers for outstanding contributions to research. Dr. Marcia McNutt is president.

The **National Academy of Engineering** was established in 1964 under the charter of the National Academy of Sciences to bring the practices of engineering to advising the nation. Members are elected by their peers for extraordinary contributions to engineering. Dr. C. D. Mote, Jr., is president.

The **National Academy of Medicine** (formerly the Institute of Medicine) was established in 1970 under the charter of the National Academy of Sciences to advise the nation on medical and health issues. Members are elected by their peers for distinguished contributions to medicine and health. Dr. Victor J. Dzau is president.

The three Academies work together as the **National Academies of Sciences, Engineering, and Medicine** to provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions. The National Academies also encourage education and research, recognize outstanding contributions to knowledge, and increase public understanding in matters of science, engineering, and medicine.

Learn more about the National Academies of Sciences, Engineering, and Medicine at [www.nationalacademies.org](http://www.nationalacademies.org).

*The National Academies of*  
SCIENCES • ENGINEERING • MEDICINE

**Consensus Study Reports** published by the National Academies of Sciences, Engineering, and Medicine document the evidence-based consensus on the study's statement of task by an authoring committee of experts. Reports typically include findings, conclusions, and recommendations based on information gathered by the committee and the committee's deliberations. Each report has been subjected to a rigorous and independent peer-review process and it represents the position of the National Academies on the statement of task.

**Proceedings** published by the National Academies of Sciences, Engineering, and Medicine chronicle the presentations and discussions at a workshop, symposium, or other event convened by the National Academies. The statements and opinions contained in proceedings are those of the participants and are not endorsed by other participants, the planning committee, or the National Academies.

For information about other products and activities of the National Academies, please visit [www.nationalacademies.org/about/whatwedo](http://www.nationalacademies.org/about/whatwedo).

## **COMMITTEE ON ENHANCING THE RESILIENCE OF THE NATION'S ELECTRIC POWER TRANSMISSION AND DISTRIBUTION SYSTEM**

M. GRANGER MORGAN, *Chair*, NAS,<sup>1</sup> Carnegie Mellon University, Pittsburgh,  
Pennsylvania  
DIONYSIOS ALIPRANTIS, Purdue University, West Lafayette, Indiana  
ANJAN BOSE, NAE,<sup>2</sup> Washington State University, Pullman  
W. TERRY BOSTON, NAE, PJM Interconnection (retired), Signal Mountain, Tennessee  
ALLISON CLEMENTS, goodgrid, LLC, Salt Lake City, Utah  
JEFFERY DAGLE, Pacific Northwest National Laboratory, Richland, Washington  
PAUL DE MARTINI, Newport Consulting, Sausalito, California  
JEANNE FOX, Columbia University, New York  
ELSA GARMIRE, Dartmouth College (retired), Santa Cruz, California  
RONALD E. KEYS, United States Air Force (retired), Woodbridge, Virginia  
MARK McGRANAGHAN, Electric Power Research Institute, Knoxville, Tennessee  
CRAIG MILLER, National Rural Electric Cooperative Association, Alexandria, Virginia  
THOMAS J. OVERBYE, Texas A&M University, College Station  
WILLIAM H. SANDERS, University of Illinois, Urbana-Champaign  
RICHARD E. SCHULER, Cornell University, Ithaca, New York  
SUSAN TIERNEY, Analysis Group, Aurora, Colorado  
DAVID G. VICTOR, University of California, San Diego

### **Staff**

K. JOHN HOLMES, Study Director  
DANA CAINES, Financial Manager  
ELIZABETH EULLER, Senior Program Assistant (until June 2016)  
JORDAN D. HOYT, Christine Mirzayan Science and Technology Policy Graduate Fellow  
LANITA JONES, Administrative Coordinator (until August 2017)  
JANKI U. PATEL, Program Assistant  
BEN A. WENDER, Program Officer  
E. JONATHAN YANGER, Research Associate (until April 2017)  
JAMES J. ZUCCHETTO, Senior Scientist

---

<sup>1</sup> NAS, National Academy of Sciences.

<sup>2</sup> NAE, National Academy of Engineering.

NOTE: See Appendix C, Disclosure of Conflicts of Interest.

**BOARD ON ENERGY AND ENVIRONMENTAL SYSTEMS**

JARED L. COHON, *Chair*, NAE,<sup>1</sup> Carnegie Mellon University, Pittsburgh, Pennsylvania  
DAVID T. ALLEN, NAE, University of Texas, Austin  
W. TERRY BOSTON, NAE, PJM Interconnection (retired), Signal Mountain, Tennessee  
WILLIAM BRINKMAN, NAS,<sup>2</sup> Princeton University, New Jersey  
EMILY A. CARTER, NAS/NAE, Princeton University, New Jersey  
BARBARA KATES-GARNICK, Tufts University, Medford, Massachusetts  
JOANN MILLIKEN, Independent Consultant, Alexandria, Virginia  
MARGO TSIRIGOTIS OGE, Environmental Protection Agency (retired), McLean, Virginia  
JACKALYNE PFANNENSTIEL,<sup>3</sup> Independent Consultant, Piedmont, California  
MICHAEL P. RAMAGE, NAE, ExxonMobil Research and Engineering Company (retired), New York  
DOROTHY ROBYN, Independent Consultant, Washington, D.C.  
GARY ROGERS, Roush Industries, Livonia, Michigan  
KELLY SIMS-GALLAGHER, Tufts University, Medford, Massachusetts  
MARK THIEMENS, NAS, University of California, San Diego  
JOHN WALL, NAE, Cummins Engine Company (retired), Belvedere, California  
ROBERT WEISENMILLER, California Energy Commission, Sacramento

**Staff**

K. JOHN HOLMES, Acting Director/Scholar  
DANA CAINES, Financial Manager  
LANITA JONES, Administrative Coordinator (until August 2017)  
MARTIN OFFUTT, Senior Program Officer  
JANKI U. PATEL, Program Assistant  
BEN A. WENDER, Program Officer  
JAMES J. ZUCCHETTO, Senior Scientist

---

<sup>1</sup> NAE, National Academy of Engineering.

<sup>2</sup> NAS, National Academy of Sciences.

<sup>3</sup> Deceased on April 26, 2017.

## Preface

Electricity and the underlying infrastructure for its production, transmission, and distribution are essential to the health and prosperity of all Americans. It is important to make investments that increase the reliability of the power system within reasonable cost constraints. However, the system is complex and vulnerable. Despite all best efforts, it is impossible to avoid occasional, potentially large outages caused by natural disasters or pernicious physical or cyber attacks. This report focuses on large-area, long-duration outages—considered herein as blackouts that last several days or longer and extend over multiple service areas or states. When such major electricity outages do occur, economic costs can tally in the billions of dollars and lives can be lost. Hence, there is a critical need to increase the resilience of the U.S. electric power transmission and distribution system—so that major outages are less frequent, their impacts on society are reduced, and recovery is more rapid—and to learn from these experiences so that performance in the future is better.

The many high-profile electric-service interruptions that have occurred over the past two decades, along with recent efforts to enhance the capabilities of the nation's electricity delivery system, prompted several observers to seek an independent review of the vulnerability and resilience of the nation's electricity delivery system. In its 2014 appropriations for the Department of Energy (DOE), Congress called for an independent assessment to “conduct a national-level comprehensive study on the future resilience and reliability of the nation's electric power transmission and distribution system. At a minimum, the report should include technological options for strengthening the capabilities of the nation's power grid; a review of federal, state, industry, and academic research and development programs; and an evaluation of cybersecurity for energy delivery systems.”<sup>1</sup>

The National Academies of Sciences, Engineering, and Medicine established the Committee on Enhancing the Resilience of the Nation's Electric Power Transmission and Distribution System to conduct the study. On the basis of this mandate, the National Academies asked the committee to address technical, policy, and institutional factors that might affect how modern technology can be implemented to improve the resilience of the electric system; recommend strategies and priorities for how this might be achieved; and identify barriers to its implementation. The full statement of task for the committee is shown in Appendix A. The biographies of the committee members that authored this report are contained in Appendix B.

Committee members included academicians, retirees from industry, current or former employees of state government agencies, and representatives of other organizations. They brought considerable expertise on the operation and regulation of electric power networks, security, and energy economics. The committee met six times in 2016 and 2017 to gather information from public sources (listed in Appendix D) and to discuss the key issues. It also held several conference calls.

The committee operated under the auspices of the National Academies of Sciences, Engineering, and Medicine's Board on Energy and Environmental Systems and is grateful for the able assistance of K. John Holmes, Linda Casola, Elizabeth Euler, Jordan Hoyt, Janki U. Patel, Ben A. Wender, E. Jonathan Yanger, and James Zucchetto of the National Academies' staff.

---

<sup>1</sup> H.R. 113-486, page 103.





## Acknowledgment of Reviewers

This Consensus Study Report was reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise. The purpose of this independent review is to provide candid and critical comments that will assist the National Academies of Sciences, Engineering, and Medicine in making each published report as sound as possible and to ensure that it meets the institutional standards for quality, objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process.

We thank the following individuals for their review of this report:

Mr. William Ball, Southern Company Services, Inc.,  
Mr. Joe Brannan, North Carolina Electric Membership Corporation,  
Dr. L. Berkley Davis, Jr. (NAE), GE Power & Water,  
Mr. Phillip Harris, Tres Amigas LLC,  
Dr. James L. Kirtley, Jr. (NAE), Massachusetts Institute of Technology,  
Dr. Butler W. Lampson (NAS/NAE), Microsoft Research,  
Mr. Ralph LaRossa, Public Service Electric & Gas Company,  
Mr. Jason McNamara, CNA,  
Ms. Diane Munns, Environmental Defense Fund,

Mr. David K. Owens, Edison Electric Institute (retired),  
Dr. William H. Press (NAS), The University of Texas, Austin  
Dr. B. Don Russell (NAE), Texas A&M University,  
Dr. Alberto Sangiovanni-Vincentelli (NAE), University of California, Berkeley,  
Dr. Edmund O. Schweitzer, III (NAE), Schweitzer Engineering Laboratories, Inc.,  
Mr. Rich Sedano, Regulatory Assistance Project, and  
Dr. Paul Stockton, Sonecon, LLC.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations of this report nor did they see the final draft before its release. The review of this report was overseen by Julia M. Phillips, NAE, Sandia National Laboratories (retired), and John G. Kassakian, NAE, Massachusetts Institute of Technology (retired). They were responsible for making certain that an independent examination of this report was carried out in accordance with the standards of the National Academies and that all review comments were carefully considered. Responsibility for the final content rests entirely with the authoring committee and the National Academies.



# Contents

SUMMARY	1
1 INTRODUCTION AND MOTIVATION	8
The Nation Depends on a Resilient Electric System, 8	
Resilience and Reliability Are Not the Same Thing, 9	
The Need for More Resilient Transmission and Distribution Systems, 10	
Improving Resilience Presents Fundamental Challenges, 12	
Structure of the Report, 15	
References, 16	
2 TODAY'S GRID AND THE EVOLVING SYSTEM OF THE FUTURE	17
Introduction, 17	
Electric Industry Structure, Asset Ownership, and Operational Roles and Responsibilities, 17	
Physical Structure and Operation of the High-Voltage Transmission Systems, 25	
Physical Structure and Operation of the Distribution System, 27	
Metrics for Reliability and Resilience, 31	
Near-Term Drivers of Change and Associated Challenges and Opportunities for Resilience, 35	
Longer-Term Drivers of Change and Associated Challenges and Opportunities for Resilience, 42	
Sustaining and Improving the Resilience of a Grid That Is Changing Rapidly and in Uncertain Ways, 47	
References, 47	
3 THE MANY CAUSES OF GRID FAILURE	50
Introduction, 50	
Different Causes Require Different Preparation and Have Different Consequences, 50	
Reviewing the Causes of Outages, 50	
The Life Cycle of a Power Outage, 66	
References, 68	
4 STRATEGIES TO PREPARE FOR AND MITIGATE LARGE-AREA, LONG-DURATION BLACKOUTS	70
Introduction, 70	
Planning and Design, 70	
Operations, 86	
References, 92	

5	STRATEGIES FOR REDUCING THE HARMFUL CONSEQUENCES FROM LOSS OF GRID POWER	94
	Introduction, 94	
	Incentives for Preparedness, 95	
	Planning for Grid Failure, 99	
	Design, 104	
	Distribution System Innovations That Could Enhance Resilience, 106	
	References, 108	
6	RESTORING GRID FUNCTION AFTER A MAJOR DISRUPTION	110
	Introduction, 110	
	General Model for Electricity Restoration, 110	
	Disruptions That Involve Across-the-Board Damage to the Grid and Its Supporting Infrastructure, 114	
	Disruptions That Involve Damage to the Cyber Monitoring and Control Systems, 119	
	Disruptions That Involve Only Physical Damage, 125	
	Disruptions That Cause Both Physical and Cyber Damage, 126	
	Opportunities to Improve Restoration, 126	
	References, 129	
	Annex Tables, 130	
7	CONCLUSIONS	134
	Overarching Insights and Recommendations, 134	
	Summary of Detailed Recommendations, 137	
	References, 141	
APPENDIXES		
A	Statement of Task	143
B	Committee Biographies	144
C	Disclosure of Conflicts of Interest	149
D	Presentations and Committee Meetings	150
E	Examples of Large Outages	152
F	Acronyms	155



## Boxes, Figures, and Tables

### BOXES

- S.1 Causes of Most Electricity System Outages, 2
- 1.1 Examples of Outages on Bulk Power Systems and Their Consequences, 13
- 2.1 Examples of Four Different Electric Operational/Reliability/Ownership Structures, 24
- 2.2 Common Distribution System Reliability Metrics, 32
- 2.3 Federal and State Policy Drivers of Change in the Electric System, 36
- 2.4 Example Comments to the Committee on Distributed Energy Resource and Microgrid Deployments Across the United States, 37
- 3.1 Summary of the Metcalf Substation Attack, 53
- 3.2 Summary of the Cyber Attack on the Ukrainian Grid, 54
- 3.3 Electromagnetic Pulse, 62
- 4.1 Financial and Operational Benefits of Distribution Automation to Chattanooga Electric Power Board, 74
- 4.2 Examples of Electric System Vulnerability to Disruptions in Natural Gas Infrastructure, 76
- 4.3 Select Regulatory Actions Supporting Hardening, Modernization, and Other Preventative Investments, 85
- 5.1 Consequences and Civic Response to Damage Caused by the Ice Storm of January 1998, 98
- 5.2 Superstorm Sandy: Preparation, Emergency Response, and Restoration of Services, 102

### FIGURES

- 1.1 The relative frequency of outages in the U.S. bulk power system over the period from 1984 to 2015, 10
- 1.2 (A) A four-stage process of resilience based on a framing by Flynn (2008) and as illustrated by NIAC (2010); (B) In the case of the hierarchically organized power system, these concepts apply at several

different levels of the system with different specific actions and lessons; and (C) Illustration of scales of resilience processes, 11

- 2.1 The bulk energy system encompasses the facilities and control systems for generation and transmission of electricity but does not include local distribution systems, 18
- 2.2 Map of electric distribution utility service territories in the continental United States, 19
- 2.3 The three large electric interconnections that span the United States, large parts of Canada, and a small part of Mexico, 20
- 2.4 The North American transmission system, 21
- 2.5 Map of regional transmission organizations' (RTO) and independent system operators' (ISO) service areas in the United States and Canada, 22
- 2.6 End consumers can choose their electricity provider in restructured states (green), while other states have suspended restructuring activities (yellow) or never initiated them (white), 22
- 2.7 North American Electric Reliability Corporation reliability coordinators are responsible for ensuring reliability across multiple utility service territories, 23
- 2.8 Fraction of customer meters with advanced meters by state in 2015, 30
- 2.9 Schematic of possible electric system configurations and interactions in the future, 38
- 2.10 Different ways in which the nature and scope of the future regulatory environment might evolve, 43
- 2.11 Different ways in which distributed resources might evolve in the future, 43
- 2.12 Under most state laws, there is legal distinction between a utility that serves a multi-story building with its own distributed energy resource and combined heat and power, as shown at the top of this figure, and the situation in which the same loads are distributed across space and are served by a small microgrid, 44
- 2.13 Climate change can affect, and be affected by, the power system, 45

- 2.14 Possible change in the sources and nature of bulk power, 46
- 3.1 Mapping of events that can cause disruption of power systems, 51
- 3.2 Illustration of distinct types of damages that can affect power systems, 52
- 3.3 U.S. Geological Survey assessment of earthquake hazard across the United States, 53
- 3.4 U.S. coastal locations that have experienced major tsunamis over the course of the past 1,000 years, 55
- 3.5 Summary of the state of knowledge of how the frequency and intensity of various weather events may evolve over time, 55
- 3.6 Map of tornado frequency from 1990 to 2009, 56
- 3.7 Tornadoes show a strong (A) temporal and (B) seasonal variation, 57
- 3.8 In 2006, a cluster of tornadoes caused damage across four states in 10 hours from one super cell, 58
- 3.9 (A) Distribution of freezing rain from 1948 to 2000, (B) slight recent trend toward more events, and (C) best estimate of trend by region, 59
- 3.10 (A) Ice accumulation of several inches on distribution lines caused these poles to collapse, and (B) images from the infamous 1998 ice storm across southeastern Canada and the northeastern United States, 60
- 3.11 Example of a Federal Emergency Management Agency flood map for the Susquehanna River near West Pittston, Pennsylvania, 61
- 3.12 (A) The region of hurricane risk is greatest on the Atlantic and Gulf coasts of the United States and (B) recent years have seen a trend of Atlantic hurricanes becoming more intense, 63
- 3.13 Volcanic hazard map for the region around Mount Rainier, 65
- 3.14 Notional time series of a major power outage divided into six stages, 67
- 4.1 The process of considering and mitigating individual component vulnerability based on cost-performance optimization, 71
- 4.2 (A) Following a major storm that disrupted service on many distribution circuits operated by Chattanooga Electric Power Board, automatic reconfiguration prevented outages for many customers (purple) and significantly reduced the number of circuits requiring manual repairs (green); and (B) such automation has greatly reduced the number of customer-hours (area under the curve) of outage experienced, 73
- 4.3 (A) Installations of utility-scale battery storage have increased substantially over the last 5 years, (B) although growth is concentrated in a few areas and dominated by lithium-ion chemistries, 75
- 4.4 2000-bus synthetic network sited in Texas, 79
- 4.5 Disruption of any material or service that the electricity system relies on can result in loss of electric service and make restoration more challenging, 83
- 4.6 Power system operating states, 86
- 4.7 ISO New England control room, 89
- 5.1 Installation of microgrids in 2015 and expected growth to 2020, 97
- 5.2 Installation of “behind the meter” battery storage systems, 97
- 6.1 Illustration of the general processes of restoration that occur on multiple levels by different institutions with responsibility for electricity restoration, 111
- 6.2 Example of data integration to support advanced data analytics for improved restoration efforts, 116
- 6.3 Three ABB single-phase 345 kV compact replacement transformers being moved from St. Louis, Missouri, to a substation in Houston, Texas, under a Department of Homeland Security demonstration project, 117
- 6.4 Restoration of industrial control systems after a cyber breach, 119

## TABLES

- 2.1 Breakdown of Utilities That Own and Operate Generation, Transmission, or Distribution Infrastructure, 19
- 2.2 Example Resilience Metrics Proposed by the Department of Energy-supported Grid Modernization Laboratory Consortium, 33
- 5.1 The Significant Variation in Estimated Financial Losses Suffered by Different Customer Classes Operating under Different Ambient Conditions as a Function of Varying Outage Duration, 96
- 5.2 The Federal Emergency Management Agency's Matrix Concept Illustrates the High Amount of Interagency and Interdepartmental Coordination Required for Assessing and Responding to Threats to the Nation's Vital Infrastructures, 101
- 6.1 Summary of Selected Recommendations Made by the National Research Council in Its 2012 Report *Terrorism and the Electric Power Delivery System*, Together with the Committee's Assessment of Where Things Now Stand, 124
- 6A.1 Variation in Restoration Activities Across the Six Stages of the Life Cycle of an Outage Characterized by Damage to Physical Components, Monitoring and Control Systems, and Supporting Infrastructure, As Indicated in the Upper Right Corner of Figure 3.2, 130
- 6A.2 Restoration Activities Across the Six Stages of the Life Cycle of an Outage from a Cyber Attack, 133

## Summary

Americans' safety, productivity, comfort, and convenience depend on the reliable supply of electric power. The electric power system is a complex "cyber-physical" system composed of a network of millions of components spread out across the continent. These components are owned, operated, and regulated by thousands of different entities. Power system operators work hard to assure safe and reliable service, but large outages occasionally happen. Given the nature of the system, there is simply no way that outages can be completely avoided, no matter how much time and money is devoted to such an effort. The system's reliability and resilience can be improved but never made perfect. Thus, system owners, operators, and regulators must prioritize their investments based on potential benefits. Most interruptions result from physical damage in a local part of the distribution system caused by weather, accidents, or aging equipment that fails. Less frequently, major storms and other natural phenomena, operations errors, and pernicious human actions can cause outages on the bulk power system (i.e., generators and high-voltage power lines) as well as on distribution systems.

### RESILIENCE IS BROADER THAN RELIABILITY

This report of the Committee on Enhancing the Resilience of the Nation's Electric Power Transmission and Distribution System focuses on identifying, developing, and implementing strategies to increase the power system's *resilience* in the face of events that can cause large-area, long-duration outages: blackouts that extend over multiple service areas or states and last several days or longer. Resilience is not just about lessening the likelihood that these outages will occur. It is also about limiting the scope and impact of outages when they do occur, restoring power rapidly afterwards, and learning from these experiences to better deal with events in the future.

The power system has been undergoing dramatic changes in technology and governance. In some parts of the United States, power is still supplied by regulated, vertically integrated utilities that generate electricity in large power plants, move that power out over high-voltage transmission systems,

and distribute it to end-use customers—all under that single utility's control. In other parts of the country, electric utilities have been restructured to promote competitive markets, particularly in wholesale power sales between generators and electricity distribution companies. In the more market-oriented parts of the country, high-voltage transmission lines that connect wholesale buyers and sellers are regulated or publicly owned, as are most distribution systems that provide the poles, wires, and equipment to serve retail customers. However, the flows over those wires and customers' responses are increasingly determined by market forces. Efforts to improve resilience must accommodate institutional and policy heterogeneity across the country.

There has been significant growth in instrumentation and automation at the level of the high-voltage, or bulk power, system. This allows the system to operate more efficiently and provides system operators with much better situational awareness; this can improve grid reliability and resilience in the face of outages, but this added complexity can also introduce cybersecurity vulnerabilities. Analogous technological advancements on distribution systems (i.e., "smart grids")—including improved sensing, communication, automation technologies, and advanced metering infrastructure—are occurring piecemeal across the country.

In some states, such as Hawaii and California, distributed energy resources, including distributed generation, demand response, energy efficiency, customer-owned storage, microgrids, and electric vehicles, are a rapidly growing fraction of the overall resource mix that must be planned and managed to maintain grid reliability, resilience, and security. However, despite these developments, for at least the next two decades, most U.S. customers will continue to depend on the functioning of the large-scale, interconnected, tightly organized, and hierarchically structured electric grid.

Strategies to enhance electric power resilience must accommodate both a diverse set of technical and institutional arrangements and a wide variety of hazards. There is no "one-size-fits-all" solution to avoiding, planning for, coping with, and recovering from major outages.

## FRAMEWORK AND ORGANIZATION

Chapter 1 provides a brief introduction to the electricity system and motivation for this report. Chapter 2 summarizes the present state of the electricity system and the various ways it may evolve in the future, as well as metrics used to monitor grid reliability and resilience. Chapter 3 identifies, discusses, and compares a range of natural hazards and accidental and pernicious human actions that could cause major disruptions in service. Many of these, listed in Box S.1, have caused outages or impacted electricity system functions at varying scales over the past 30 years, either in the United States or globally. Others hold the potential to become major causes of disruption in the future.

Building a strategy to increase system resilience requires an understanding of a wide range of preparatory, preventative, and remedial actions, as well as how these impact planning, operation, and restoration over the entire life cycle of different kinds of grid failures. Strategies must be crafted with awareness and understanding of the temporal arc of a major outage, as well as how the needs differ from one type of event to another. It is also important to differentiate between actions designed to make the grid more robust and resilient to failure (e.g., wind-resistant steel or concrete poles rather than wood poles) and those that improve the effectiveness of recovery (e.g., preemptively powering down some pieces of the system to minimize damage). Some actions serve both strategies, some serve one but not the other, and some serve one while inhibiting the other. Similarly, the timing of repairs is different depending on the cause. For example, repairs can begin immediately after a tornado has passed, but flooding following a hurricane can delay the start of repair and impede repair efforts. Good planning and preparation are essential to mitigating, coping with, and recovering from major outages. Both human and technical systems must be designed before grid failure so that the responders can assess the extent of failure and damage, dispatch resources effectively, and draw on established component inventories, supply chains, crews, and communication channels.

## Anticipating and Preparing for Disruption

While the possibility of large-area, long-duration blackouts cannot be totally eliminated, there is much that can be done to decrease their likelihood and reduce their magnitude, should they occur. Chapter 4 assesses a variety of techniques that can be employed before an event occurs in order to enhance system resilience. These include improving the health and reliability of the individual grid components (e.g., through asset health monitoring and preventive- and reliability-centered maintenance), improving system architectures to further reduce the criticality of individual components, better simulating high-impact events, and considering the criticality of the grid's underlying cyber infrastructure. Further work can be done in the area of real-time operations to enhance resilience. This includes improving situational awareness in the control room, with a focus on severe events and an inclusion of the cyber infrastructure, adding more wide-area monitoring and control, and developing control systems that better tolerate both accidental faults and malicious attacks. Finally, there is a need to deal with myriad regulatory entities and incentives to fund resilience investments.

## Mitigating the Impacts of Disruption

While large failures of the bulk power system are rare, some will occur, and restoration can take a long time. It is essential that society prepare for periods of prolonged outage, because many vital public infrastructures—such as heating and cooling, water and sewage pumping, traffic control, financial systems, and many aspects of emergency response and public security—depend on the electric power supply. These issues are explored in Chapter 5. The effects of power outages vary with weather, for different types and locations of users, and over different durations. A central theme of this report is the need to improve how different elements of society perform the difficult task of imagining

### BOX S.1

#### Causes of Most Electricity System Outages (shown in alphabetical order and reviewed in Chapter 3)

Cyber attacks	Hurricanes	Space weather and other electromagnetic threats
Drought and water shortage	Ice storms	Tsunamis
Earthquakes	Major operations errors	Volcanic events
Floods and storm surge	Physical attacks	Wildfires
	Regional storms and tornadoes	

## SUMMARY

the diverse consequences of prolonged power outages. Also important is to ensure that equipment that has been purchased or contracted for backup power supply will be available and reliable when needed.

### Recovering from and Learning after Disruption

After the bulk power system has failed, first responders, utilities, and public agencies must work together to restore service. Recovery involves coordinated activity on the physical side—for example, repairing, replacing, and reconfiguring the hardware of the grid—as well as a variety of activities to rebuild the cyber and industrial control systems. These issues are the focus of Chapter 6. Effective restoration must begin well before the disaster through numerous preparatory activities, including drills and stockpiling of key equipment. Utilities and other electric service personnel must think about how they will assess damage, plan restoration, and marshal and deploy the necessary resources. This is complicated by the fact that restoration processes are starkly different depending on the nature of the event. The keys to restoration are to envision a broad range of threats, work through failure scenarios, plan, and rehearse. Regardless of the cause of the outage, restoration always involves agility, collaboration and communications across multiple institutions, and an understanding of the state of the grid and its supporting systems. Technical readiness is the ultimate determinant of the ability to restore, but technical readiness rests firmly on organizational readiness. A process of continual learning and improvement, informed by detailed incident investigations following large outages, is essential for enhancing the resilience of the grid.

### OVERARCHING INSIGHTS AND RECOMMENDATIONS

No single entity is responsible for, or has the authority to implement, a comprehensive approach to assure the resilience of the nation's electricity system. Because most parties are preoccupied dealing with short-term issues, they neither have the time to think systematically about what could happen in the event of a large-area, long-duration blackout, nor adequately consider the consequences of large-area, long-duration blackouts in their operational and other planning or in setting research and development priorities. Hence the United States needs a process to help all parties better envision the consequences of low-probability but high-impact events precipitated by the causes outlined in Chapter 3 and the system-wide effects discussed in Chapter 5. The specific recommendations addressed to particular parties that are provided throughout the report (especially in Chapters 4 through 6) will incrementally advance the cause

of resilience. However, these alone will be insufficient unless the nation is able to adopt a more integrated perspective at the same time. Hence, in addition to the report's *specific* recommendations, the committee provides a series of overarching recommendations.

One of the best ways to make sure that things already in place will work when they are needed is to conduct drills with other critical infrastructure operators through large-scale, multisector exercises. Such exercises can help illuminate areas where improvements in processes and technologies can substantively enhance the resilience of the nation's critical infrastructure.

**Overarching Recommendation 1:** Operators of the electricity system, including regional transmission organizations, investor-owned utilities, cooperatives, and municipally owned utilities, should work individually and collectively, in cooperation with the Electricity Subsector Coordinating Council, regional and state authorities, the Federal Energy Regulatory Commission, and the North American Electric Reliability Corporation, to conduct more regional emergency preparedness exercises that simulate accidental failures, physical and cyber attacks, and other impairments that result in large-scale loss of power and/or other critical infrastructure sectors—especially communication, water, and natural gas. Counterparts from other critical infrastructure sections should be involved, as well as state, local, and regional emergency management offices.

The challenges that remain to achieving grid resilience are so great that they cannot be achieved by research- or operations-related activities alone. While new technologies and strategies can improve the resilience of the power system, many existing technologies that show promise have yet to be fully adopted or implemented. In addition, more coordination between research and implementation activities is needed, building on the specific recommendations made throughout this report. Immediate action is needed both to implement available technological and operational changes and to continue to support the development of new technologies and strategies.

**Overarching Recommendation 2:** Operators of the electricity system, including regional transmission organizations, investor-owned utilities, cooperatives, and municipals, should work individually and collectively to more rapidly implement resilience-enhancing technical capabilities and operational strategies that are available today and to speed the adoption of new capabilities and strategies as they become available.

The Department of Energy (DOE) is the federal entity with a mission to focus on the *longer-term* issues of



developing and promulgating technologies and strategies to increase the resilience and modernization of the electric grid.<sup>1</sup> No other entity in the United States has the mission to support such work, which is critical as the electricity system goes through the transformational changes described in this report. The committee views research, development, and demonstration activities that support reliable and resilient electricity systems to constitute a public good. If funding is not provided by the federal government, the committee is concerned that this gap would not be filled either by states or by the private sector. In part this is because the challenges and solutions to ensuring grid resilience are complex, span state and even national boundaries, and occur on time scales that do not align with business models. At present, two offices within DOE have responsibility for issues directly and indirectly related to grid modernization and resilience.

**Overarching Recommendation 3:** However the Department of Energy chooses to organize its programs going forward, Congress and the Department of Energy leadership should sustain and expand the substantive areas of research, development, and demonstration that are now being undertaken by the Department of Energy's Office of Electricity Delivery and Energy Reliability and Office of Energy Efficiency and Renewable Energy, with respect to grid modernization and systems integration, with the explicit intention of improving the resilience of the U.S. power grid. Field demonstrations of physical and cyber improvements that could subsequently lead to widespread deployment are critically important. The Department of Energy should collaborate with parties in the private sector and in states and localities to jointly plan for and support such demonstrations. Department of Energy efforts should include engagement with key stakeholders in emergency response to build and disseminate best practices across the industry.

The U.S. grid remains vulnerable to natural disasters, physical and cyber attacks, and other accidental failures.

**Overarching Recommendation 4:** Through public and private means, the United States should substantially increase the resources committed to the physical components needed to ensure that critical electric infrastructure is robust and that society is able to cope when the grid fails. Some of this investment should focus on making the existing infrastructure more resilient and easier to repair, including the following:

- The Department of Energy should launch a program to manufacture and deploy flexible and transportable three-phase recovery transformer sets that can be pre-positioned around the country.<sup>2</sup> These recovery transformers should be easy to install and use temporarily until conventional transformer replacements are available. This effort should produce sufficient numbers (on the order of tens compared to the three produced by the Department of Homeland Security's RecX program) to provide some practical protection in the case of an event that results in the loss of a number of high-voltage transformers. This effort should complement, instead of replace, ongoing initiatives related to spare transformers.
- State and federal regulatory commissions and regional transmission organizations should then evaluate whether grids under their supervision need additional pre-positioned replacements for critical assets that can help accelerate orderly restoration of grid service after failure.
- Public and private parties should expand efforts to improve their ability to maintain and restore critical services—such as power for hospitals, first responders, water supply and sewage systems, and communication systems.<sup>3</sup>
- The Department of Energy, the Department of Homeland Security, the Electricity Subsector Coordinating Council, and other federal organizations, such as the U.S. Army Corps of Engineers, should oversee the development of more reliable inventories of backup power needs and capabilities (e.g., the U.S. Army Corps of Engineers' mobile generator fleet), including fuel supplies. They should also "stress test" existing supply contracts for equipment and fuel supply that are widely used in place of actual physical assets in order to be certain these arrangements will function in times of major extended outages. Although the federal government cannot provide backup power equipment to everyone affected by a large-scale outage, these

<sup>2</sup> As noted in Chapters 6 and 7, the Department of Energy's Office of Electricity Delivery and Energy Reliability is supporting the development of a new generation of high-voltage transformers that will use power electronics to adjust their electrical properties and hence can be deployed in a wider range of settings. The committee's recommendation to manufacture recovery transformers is not intended to replace that longer-term effort. However, the Department of Energy's new advanced transformer designs will not be available for some time; in the meantime, the system remains physically vulnerable. While in Chapter 6 the committee notes several government and industry-led transformer sharing and recovery programs, it recognizes that high-voltage transformers represent one of the grid's most vulnerable components deserving of further efforts.

<sup>3</sup> In addition to treatment, sewage systems often need to pump uphill. A loss of power can quickly lead to sewage backups. Notably, a high percentage of the hospital backup generators in New York City failed during Superstorm Sandy.

<sup>1</sup> The Department of Homeland Security, the Federal Energy Regulatory Commission, and other organizations also provide critical support and have primacy in certain areas.

## SUMMARY

resources could make significant contributions at select critical loads.

In addition to providing redundancy of critical assets, transmission and distribution system resilience demands the ability to provide rapid response to events that impair the ability of the power system to perform its function. These events include deliberate attacks on and accidental failures of the infrastructure itself, as well as other causes of grid failure, which are discussed in Chapter 3.

**Overarching Recommendation 5:** The Department of Energy, together with the Department of Homeland Security, academic research teams, the national laboratories, and companies in the private sector, should carry out a program of research, development, and demonstration activities to improve the security and resilience of cyber monitoring and controls systems, including the following:

- Continuous collection of diverse (cyber and physical) sensor data;
- Fusion of sensor data with other intelligence information to diagnose the cause of the impairment (cyber or physical);
- Visualization techniques needed to allow operators and engineers to maintain situational awareness;
- Analytics (including machine learning, data mining, game theory, and other artificial intelligence-based techniques) to generate real-time recommendations for actions that should be taken in response to the diagnosed attacks, failures, or other impairments;
- Restoration of control system and power delivery functionality and cyber and physical operational data in response to the impairment; and
- Creation of post-event tools for detection, analysis, and restoration to complement event prevention tools.

Because no single entity is in charge of planning the evolution of the grid, there is a risk that society may not adequately anticipate and address many elements of grid reliability and resilience and that the risks of this system-wide failure in preparedness will grow as the structure of the power industry becomes more atomized and complex. There are many opportunities for federal leadership in anticipating potential system vulnerabilities at a national level, but national solutions are then refined in light of local and regional circumstances. Doing this requires a multistep process, the first of which is to anticipate the myriad ways in which the system might be disrupted and the many social, economic, and other consequences of such disruptions. The second is to envision the range of technological and organizational innovations that are affecting the industry (e.g., distributed generation and storage) and how such developments may affect the system's reliability and resilience. The

third is to figure out what upgrades should be made and how to cover their costs. For simplicity, the committee will refer to this as a "visioning process." While the Department of Homeland Security (DHS) has overarching responsibility for infrastructure protection, DOE, as the sector-specific agency for energy infrastructure, has a legal mandate and the deep technical expertise to work on such issues.

**Overarching Recommendation 6:** The Department of Energy and the Department of Homeland Security should jointly establish and support a "visioning" process with the objective of systematically imagining and assessing plausible large-area, long-duration grid disruptions that could have major economic, social, and other adverse consequences, focusing on those that could have impacts related to U.S. dependence on vital public infrastructures and services provided by the grid.

Because it is inherently difficult to imagine systematically things that have not happened (Fischhoff et al., 1978; Kahneman, 2011), exercises in envisioning benefit from having multiple groups perform such work independently. For example, such a visioning process might be accomplished through the creation of two small national power system resilience assessment groups (possibly at DOE national laboratories and/or other federally funded research and development centers or research universities). However such visioning is accomplished, engagement from staff representing relevant state and federal agencies is essential in helping to frame and inform the work. These efforts can build on the detailed recommendations in this report to identify technical and organizational strategies that increase electricity system resilience in numerous threat scenarios and to assess the costs and financing mechanisms to implement the proposed strategies. Attention is needed not just to the average economy-wide costs and benefits, but also to the distribution of these across different levels of income and vulnerability. It is important that these teams work to identify common elements in terms of hazards and solutions so as to move past a hazard-by-hazard approach to a more systems-oriented strategy. Producing useful insights from this process will require mechanisms to help these groups identify areas of overlap while also characterizing the areas of disagreement. A consensus view could be much less helpful than a mapping of uncertainties that can help other actors—for example, state regulatory commissions and first responders—understand the areas of deeper unknowns.

Of course national laboratories, other federally funded research and development centers, and research universities do not operate or regulate the power system. At the national level, the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) both have relevant responsibilities and authorities.

**Overarching Recommendation 7A:** The Federal Energy Regulatory Commission and the North American Electric Reliability Corporation should establish small system resilience groups, informed by the work of the Department of Energy/Department of Homeland Security “visioning” process, to assess and, as needed, to mandate strategies designed to increase the resilience of the U.S. bulk electricity system. By focusing on the crosscutting impacts of hazards on interdependent critical infrastructures, one objective of these groups would be to complement and enhance existing efforts across relevant organizations.

As the discussions throughout this report make clear, many different organizations are involved in planning, operating, and regulating the grid at the local and regional levels. By design and of necessity in our constitutional democracy, making decisions about resilience is an inherently political process. Ultimately the choice of how much resilience our society should and will buy must be a collective social judgment. It is unrealistic to expect firms to make investments voluntarily whose benefits may not accrue to shareholders within the relevant commercial lifetime for evaluating projects. Moreover, much of the benefit from avoiding such events, should they occur, will not accrue to the individual firms that invest in these capabilities. Rather, the benefits are diffused more broadly across multiple industries and society as a whole, and many of the decisions must occur on a state-by-state basis.

**Overarching Recommendation 7B:** The National Association of Regulatory Utility Commissioners should work with the National Association of State Energy Officials to create a committee to provide guidance to state regulators on how best to respond to identified local and regional power system-related vulnerabilities. The work of this committee should be informed by the national “visioning” process, as well as by the work of other research organizations. The mission of this committee should be to develop guidance for, and provide technical and institutional support to, state commissions to help them to more systematically address broad issues of power system resilience, including decisions as to what upgrades are desirable and how to pay for them. Guidance developed through this process should be shared with appropriate representatives from the American Public Power Association and the National Rural Electric Cooperative Association.

**Overarching Recommendation 7C:** Each state public utility commission and state energy office, working with the National Association of Regulatory Utility Commissioners, the National Association of State Energy Officials, and state and regional grid operators and emergency preparedness organizations, should establish a standing capability to identify vulnerabilities, identify strategies to reduce local vulnerabilities, develop strategies to cover costs of needed

upgrades, and help the public to become better prepared for extended outages. In addition, they should encourage local and regional governments to conduct assessments of their potential vulnerabilities in the event of large-area, long-duration blackouts and to develop strategies to improve their preparedness.

Throughout this report, the committee has laid out a wide range of actions that different parties might undertake to improve the resilience of the United States power system. If the approaches the committee has outlined can be implemented, they will represent a most valuable contribution. At the same time, the committee is aware that the benefits of such actions—avoiding large-scale harms that are rarely observed—are easily eclipsed by the more tangible daily challenges, pressures on budgets, public attention, and other scarce resources. Too often in the past, the United States has made progress on the issue of resilience by “muddling through” (Lindblom, 1959). Even if the broad systematic approach outlined in this report cannot be fully implemented immediately, it is important that relevant organizations develop analogous strategies so that when a policy window opens in the aftermath of a major disruption, well-conceived solutions are readily available for implementation (Kingdon, 1984).

## SPECIFIC RECOMMENDATIONS

The committee assessed potential threats to the grid, and the conditions on the grid, and provides findings and recommendations throughout the report. In Chapter 7, these specific recommendations are summarized and sorted in terms of the issues they address and the entities to which they are directed. The high-level descriptions of each are listed below. The specific actions that should be taken to implement each one are laid out in Chapter 7.

**Recommendation 1 to DOE:** Improve understanding of customer and societal value associated with increased resilience and review and operationalize metrics for resilience. (Recommendations 2.1 and 2.2)

**Recommendation 2 to DOE:** Support research, development, and demonstration activities to improve the resilience of power system operations and recovery by reducing barriers to adoption of innovative technologies and operational strategies. (Recommendations 4.1, 4.6, 6.5, and 6.7)

**Recommendation 3 to DOE:** Advance the safe and effective development of distributed energy resources and microgrids. (Recommendations 4.2, 5.6, 5.12, and 6.3)

**Recommendation 4 to DOE:** Work to improve the ability to use computers, software, and simulation to research, plan, and operate the power system to increase resilience. (Recommendations 4.3, 4.4, 4.8, 4.9, and 6.12)

## SUMMARY

**Recommendation 5 to DOE:** Work to improve the cyber-security and cyber resilience of the grid. (Recommendations 4.10 and 6.8)

**Recommendation 6 to the electric power sector and DOE:** The owners and operators of electricity infrastructure should work closely with DOE in systematically reviewing previous outages and demonstrating technologies, operational arrangements, and exercises that increase the resilience of the grid. (Recommendations 4.5, 5.10, 6.2, 6.4, and 6.14)

**Recommendation 7 to DHS and DOE:** Work collaboratively to improve preparation for, emergency response to, and recovery from large-area, long-duration blackouts. (Recommendations 3.2, 5.3, 5.5, 6.1, 6.6, and 6.9)

**Recommendation 8 to DHS and DOE:** With growing awareness of the electricity system as a potential target for malicious attacks using both physical and cyber means, DHS and DOE should work closely with operating utilities and other relevant stakeholders to improve physical and cyber security and resilience. (Recommendations 3.1, 6.10, 6.11, and 6.13)

**Recommendation 9 to state offices and regulators:** Work with local utilities and relevant stakeholders to assess readiness of backup power systems and develop strategies to increase investments in resilience enhancing technologies. (Recommendations 5.1, 5.7, 5.9, and 5.11)

**Recommendation 10 to the National Association of Regulatory Utility Commissioners and federal organizations:** Work with DHS and DOE to develop guidance regarding potential social equity implications of resilience investments as well as selective restoration. (Recommendations 5.2, 5.4, and 5.8)

**Recommendation 11 to FERC and the North American Energy Standards Board:** FERC, which has regulatory authority over both natural gas and electricity systems, should address the growing risk of interdependent infrastructure. (Recommendation 4.7)

**Recommendation 12 to NERC:** Review and improve incident investigation processes to better learn from outages that happen and broadly disseminate findings and best practices. (Recommendation 6.15)

## REFERENCES

- Fischhoff, B., P. Slovic, and S. Lichtenstein. 1978. Fault trees: Sensitivity of estimated failure probabilities to problem representation. *Journal of Experimental Psychology: Human Perception and Performance* 4: 342–355.
- Kahneman, D. 2011. *Thinking Fast and Slow*. New York: Farrar, Straus, and Giroux.
- Kingdon, J.W. 1984. *Agendas, Alternatives, and Public Policies*. Boston: Little, Brown, and Company.
- Lindblom, C.E. 1959. The science of muddling through. *Public Administration Review* 19(2): 79–88.

## 1

## Introduction and Motivation

### THE NATION DEPENDS ON A RESILIENT ELECTRIC SYSTEM

The modern world runs on electricity. As individuals, we depend on electricity to heat, cool, and light our homes; refrigerate and prepare our food; pump and purify our water; handle sewage; and support most of our communications and entertainment. As a society, we depend on electricity to light our streets; control the flow of traffic on the roads, rails, and in the air; operate the myriad physical and information supply chains that create, produce, and distribute goods and services; maintain public safety, and help assure our national security.

The incredibly complex system that delivers electricity in the United States was built up gradually. It started with numerous small local systems in the early 1880s and grew to become three large independent synchronous systems<sup>1</sup> that together span the lower 48 United States, much of Canada, and some of Mexico, each of which is one of the largest integrated machines in the world. These interconnected grids have achieved significant gains in efficiency with increasing scale, as well as improved reliability owing to redundant paths over which electricity can flow. Today, power plants using fossil fuels, nuclear energy, and renewable resources supply these machines. They move power to consumers over hundreds of thousands of miles of high-voltage transmission lines and thousands more miles of local distribution lines.

While our society is becoming ever more dependent upon electricity, the electric system is undergoing a complex transformation that includes changing the mix of generation technologies; adding small-scale energy resources connected to the distribution system; incorporating generation and storage on customers' premises; and improving the capability to monitor and control electricity generation, flows, and uses.

While major pollution-control investments and activities have reduced the electric system's environmental impacts over the past century, these impacts remain a problem locally and globally. The need for environmental improvement will continue to be a major force shaping the power system for decades to come. Not only will the electric system continue to shift to a lower-carbon resource mix, but this lower-emission electricity will also be called upon to provide energy to activities, such as transportation and industrial processing, that currently operate on fossil fuels.

Our economy and lifestyles require that electricity be accessible, affordable, reliable, and continuously available. For that to happen, the grid<sup>2</sup> must perform at two levels: (1) The network of high-voltage power lines that spans the country must be able to move power from large generating plants out to local regions; and (2) Lower-voltage distribution systems must be able to move the power to, and occasionally from, factories, businesses, homes, and other end users. The grid must continue to perform these actions as it evolves to accommodate increasing numbers of distributed energy resources, which are often customer-owned, attached to local distribution systems, and have more "smart" technology—the ability to sense and interact with conditions on the grid and with customers' usage patterns and preferences. These many changes are introducing large shifts in the way the system operates. And these changes are occurring during a period of flat or declining growth in electricity generation (EIA, 2016).

For at least the next several decades, few electricity consumers, let alone whole communities, will go completely "off grid." Many consumers will install equipment that meets their needs for at least some of the time. Sometimes they will

<sup>1</sup> As explained in Chapter 2, the U.S. portions of these systems are divided into three interconnections: Eastern, Western, and Texas. Within each interconnection, 60 Hz power is synchronized across the entire system.

<sup>2</sup> Some use "the grid" only to refer to the high-voltage transmission system. Others use "the grid" to refer to the entire system of wires that moves electricity, including the lower-voltage distribution system. In this report, the committee adopts the latter usage. Chapter 2 provides an overview of the physical structure, operation, and governance of both the high-voltage transmission and lower-voltage distribution systems.



## INTRODUCTION AND MOTIVATION

also want to sell surplus power back to the grid. But the fraction of consumers who are able to provide their own resilient electric supply in entirety, without connecting to the grid, will be limited for both economic and social equity reasons.

**Finding:** For at least the next two decades, most customers will continue to depend on the functioning of the large-scale, interconnected, tightly organized, and hierarchically structured electric grid for resilient electric service.

In this context, interruptions in the power supply are disruptive for consumers and for the electric system itself. Interruptions typically arise from physical damage in a local part of the system—for example, lightning strikes, trees that fall on wires, cars or trucks that crash into power poles, or aging equipment that fails. Indeed the majority of the outages that affect the typical customer in the United States in any given year are the result of events that occur to the distribution system. Less frequently, large storms, other natural phenomena, and operator errors cause outages across the large high-voltage, or “bulk power,” system.

A wide variety of events—hurricanes, ice storms, droughts, earthquakes, wildfires, solar storms, and vandalism or malicious attacks on the hardware and software elements of the electric system—can lead to outages. When the power goes out, life becomes difficult. Communications, business operations, and traffic control all become more challenging. If the outage is brief, most people and organizations can and do cope. As the duration and spatial extent of an electricity system outage increase, costs and inconveniences grow. Critical social services—such as medical care, police and other emergency services, and communications systems—can be disrupted and lives can be lost.

This report is about minimizing the adverse impacts of large electric outages through building a resilient electric system.<sup>3</sup> A complex modern economy that depends on reliable electric supply requires a resilient electric system. While any outage can be problematic, in this report the committee focuses on large-area, long-duration outages—blackouts that last several days or longer and extend over multiple service areas or states.

## RESILIENCE AND RELIABILITY ARE NOT THE SAME THING

While utilities work hard to prevent large-scale outages, and to lessen their extent and duration, such outages do occur and cannot be eliminated. Given the many potential

sources of disruption to the power system, what is perhaps surprising is not that large outages occur, but that they are not more common. For decades, the planners and operators of the system have taken care to assure that the electric system is engineered and routinely operated to achieve high levels of reliability. Increasingly, the system’s planners and operators are focusing on resilience as well.

The North American Electric Reliability Corporation (NERC)—the federally approved organization responsible for developing reliability standards for the bulk power system—defines *reliability* in terms of two core concepts:

1. *Adequacy.* The ability of the electricity system to supply the aggregate electrical demand and energy requirements of the end-use customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements.
2. *Operating reliability.* The ability of the bulk power system to withstand sudden disturbances, such as electric short circuits or the unanticipated loss of system elements from credible contingencies, while avoiding uncontrolled cascading blackouts or damage to equipment.<sup>4</sup>

In practice, the system is planned and operated to varying reliability standards. The bulk power system achieves a relatively high degree of reliability across the United States as a whole. For example, adequacy of electricity generation capability is usually measured against a one-day-in-ten-years (1-in-10) loss of load standard, which is typically interpreted to mean that the generation reserves must be high enough that voluntary load shedding due to inadequate supply would occur only once in 10 years (Pfeifenberger et al., 2013). By its very nature, however, the highly complex electrical system—the very epitome of a “cyber-physical system”<sup>5</sup>—is spread out all across the continent. Because it is built up

<sup>4</sup> NERC goes on to state, “Regarding adequacy, system operators can and should take controlled actions or procedures to maintain a continual balance between supply and demand within a balancing area. These actions include: Public appeals; Interruptible demand (i.e., customer demand that, in accordance with contractual arrangements, can be interrupted by direct control of the system operator or by action of the customer at the direct request of the system operator); Voltage reductions (also referred to as “brownouts” because lights dim as voltage is lowered); and Rotating blackouts (i.e., the term used when each set of distribution feeders is interrupted for a limited time, typically 20–30 minutes, and then those feeders are put back in service and another set is interrupted, and so on, rotating the outages among individual feeders). All other system disturbances that result in the unplanned or uncontrolled interruption of customer demand, regardless of cause, fall under the heading of operating reliability. When these interruptions are contained within a localized area, they are considered unplanned interruptions or disturbances. When they spread over a wide area of the grid, they are referred to as cascading blackouts—the uncontrolled successive loss of system elements triggered by an incident at any location” (NERC, 2013).

<sup>5</sup> The National Science Foundation describes “cyber-physical systems” as “engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components” (NSF, 2016).

<sup>3</sup> In parallel with the preparation of this report, which was requested by the Department of Energy (DOE), DOE has also been sponsoring a 3-year Grid Modernization Initiative. That initiative includes a project to develop metrics to measure progress on grid modernization. It is pilot-testing metrics on reliability, resilience, flexibility, sustainability, affordability, and security (DOE, 2015; GMLC, 2016). This report focuses specifically on the issue of resilience.

from millions of complex physical, communications, computational, and networked components and systems, there is simply no way it can be made perfectly reliable.

The concepts of reliability differ from *resilience*, which is the focus of this report. *The Random House Dictionary of the English Language* defines resilient as follows: “the power or ability to return to the original form, position, etc. after being bent, compressed, or stretched . . . [the] ability to recover from illness, depression, adversity, or the like . . . [to] spring back, rebound.” Resilience is not just about being able to lessen the likelihood that outages will occur, but also about managing and coping with outage events as they occur to lessen their impacts, regrouping quickly and efficiently once an event ends, and learning to better deal with other events in the future. Also, a detailed analysis of failure data (Figure 1.1) reveals additional insights that will be explored further in the subsequent chapters of this report.

Flynn (2008) has outlined a four-stage framing of the concept of resilience: (1) preparing to make the system as robust as possible in the face of possible future stresses or attacks; (2) relying on resources to manage and ameliorate the consequences of an event once it has occurred; (3) recovering as quickly as possible once the event is over; and (4) remaining alert to insights and lessons that can be drawn (through all stages of the process) so that if and when another event occurs, a better job can be done in all stages.

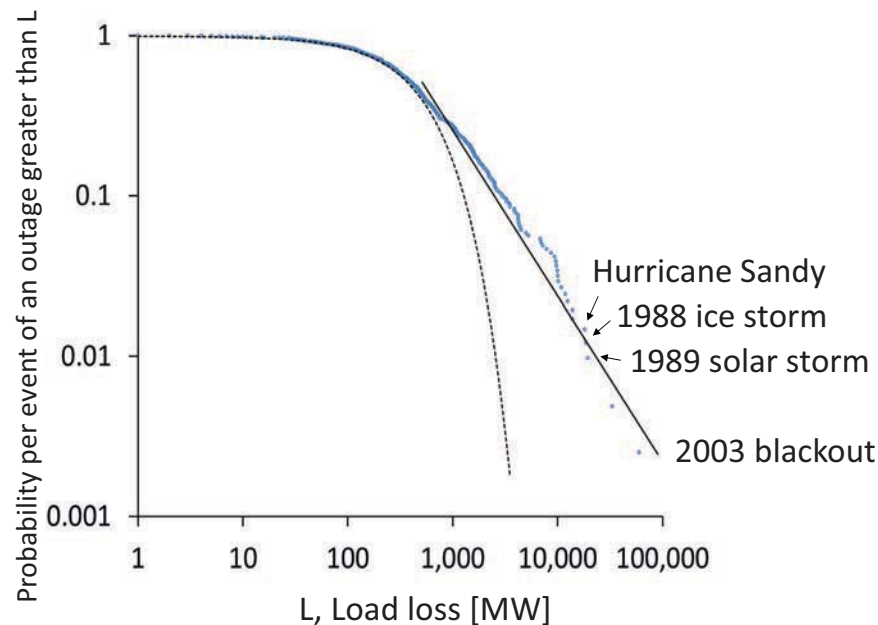
The National Infrastructure Advisory Council created a diagram that illustrates this framing (NIAC, 2010). The committee has adopted this diagram, modifying it only slightly

to add verbs at each stage (Figure 1.2A), and has structured this report to follow these stages. Because the power system is hierarchical, these same concepts apply at several different levels of the system, including at the interconnection, region (some of which are operated by regional transmission organizations), local transmission and distribution systems (typically the domain of utilities), and the end-use level (on the customer side of the meter). Figure 1.2B shows this hierarchy in the abstract, and Figure 1.2C illustrates it for the Western Interconnection. While these figures display a physical hierarchy, there is an analogous hierarchy, but with different boundaries, for the information systems that support sensing and provide control.

**Finding:** Resilience is not the same as reliability. While minimizing the likelihood of large-area, long-duration outages is important, a resilient system is one that acknowledges that such outages can occur, prepares to deal with them, minimizes their impact when they occur, is able to restore service quickly, and draws lessons from the experience to improve performance in the future.

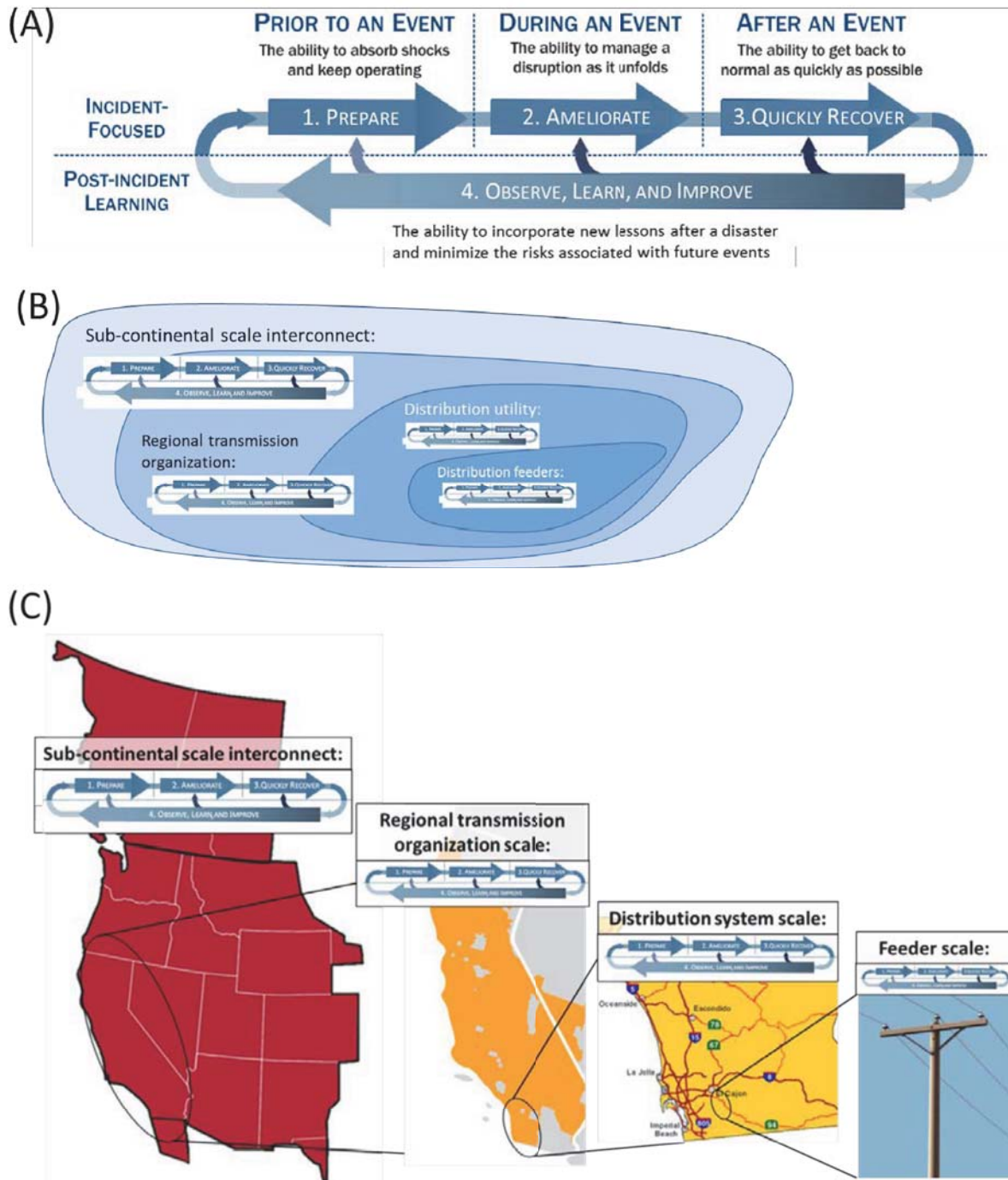
### THE NEED FOR MORE RESILIENT TRANSMISSION AND DISTRIBUTION SYSTEMS

As the committee elaborates in the chapters that follow, the 21st century power system in the United States is not just technically complicated; it is also comprised of diverse and often overlapping institutions and actors. Across the United



**FIGURE 1.1** The relative frequency of outages in the U.S. bulk power system over the period from 1984 to 2015. The figure includes 1,002 events with load loss (loss in electricity demand) greater than 1 MW. The dashed line fits an exponential distribution to the more frequent events with load loss below 500 MW. Note that large outage events do not fit this line and are much more common than one might expect from an extrapolation of the frequency of smaller events. SOURCE: Data are from EIA (2000–2015), NERC (2000–2009), and NRC (2012).

## INTRODUCTION AND MOTIVATION



**FIGURE 1.2** (A) A four-stage process of resilience based on a framing by Flynn (2008) and as illustrated by NIAC (2010); (B) In the case of the hierarchically organized power system, these concepts apply at several different levels of the system with different specific actions and lessons; and (C) Illustration of scales of resilience processes. SOURCE: Modified with permission from NIAC (2010).

States, there are differences in the resilience threats faced by power system operators, in the resources dedicated to mitigating them, and in the capabilities available to utilities and other grid operators in restoring their systems after an outage event. These variations play out in numerous ways. For example, some regions have a single grid operator that

administers competitive wholesale power markets and reliability functions. In other parts of the country, individual utilities dispatch and balance power supplies on their own in response to changing demand. In some states, there are multiple market participants (e.g., generating companies, “wires” companies that transmit power, marketing companies). In

other states, the utilities remain vertically integrated with the same firm having responsibility for both power delivery and generation. Some areas have seen the reliable introduction of many new and different pieces of electrical equipment (e.g., small-scale solar panels, large wind turbines, flywheel storage systems, large-scale electric generating power plants) owned by parties other than the utility or the local grid operator. Other regions are just beginning to manage such changes on the system.

Some utilities have embraced high-speed information and communications technologies to provide them with greater awareness of the state of their system, including the location of outages, while others have made fewer investments in such technologies. Some utilities have substantial resources dedicated to improving cybersecurity while others have close to none. As noted earlier, it is NERC's responsibility to set minimum reliability requirements to address the risks associated with the "weakest link" in the bulk power system. As discussed in more detail in Chapter 2, there is much more variability among states in terms of reliability standards, with individual states setting their own reliability requirements through public utility commissions (and boards for publicly or customer-owned distribution utilities).

Over the past 30 years, numerous headline-making outages have resulted from diverse human and natural causes, including operational errors and meteorological events. A few such outages disrupted electricity service to more than 10,000 MW of customer load (demand).<sup>6</sup> The events that cause outages of this scale leave millions of customers without power, result in economic damages<sup>7</sup> estimated in the billions of dollars, pose serious threats to health and public safety, and could potentially compromise national security. While the United States has fortunately not experienced a major outage caused by a physical or cyber attack, both are a serious and growing risk. Regarding cyber attacks, many attempts to penetrate the system occur every day. Box 1.1 describes four large-area, long-duration outage events that occurred in the past two decades in North America, ranging from the January 1998 ice storm that affected the interconnected power systems in the Northeast United States and

Eastern Canada, to the impacts resulting from Superstorm Sandy in 2012.<sup>8</sup> Box 1.1 also includes description of a cyber attack that disrupted service on the Ukrainian power system in 2015, which did not result in a large-area, long-duration outage but is noteworthy as one of the most prominent examples of cyber disruption of electricity infrastructure. As Box 1.1 makes clear, there is a wide variety of human and natural causes of outages, with significant impacts on economic and human quality of life.

**Finding:** Large-area, long-duration electricity outages that leave millions of customers without power can result in billions of dollars of economic and other damages and cause risk of injury or death. A variety of human and natural events can cause outages with a variety of consequences. The risks of physical or cyber attacks pose a serious and growing threat.

An all-hazards approach to resilience planning is essential, but, with the exception of a few general strategies, there is no "one-size-fits-all" solution to planning for and recovering from major outages. The notion of resilience has to address multiple types of events and operate in a system with multiple overlapping institutions, service providers, grid configurations, ownership structures, and regulatory systems. As outlined above, the system is also comprised of multiple and changing technologies and is constantly evolving. Together this complex physical–cyber–social system is the context and motivation for the National Academies' study presented here.

## IMPROVING RESILIENCE PRESENTS FUNDAMENTAL CHALLENGES

Throughout this report, the committee identifies and discusses a range of technical, institutional, and other strategies that, if adopted, could significantly increase the resilience of the U.S. electric power transmission and distribution systems. It is relatively easy to identify actions and strategies that could improve resilience. Much harder, however, is fostering and realizing the political and organizational support to implement these strategies and actions. The very structure of governance and investment in the electric grid is decentralized. And investment in the grid competes with other social and economic demands as well as for the time and attention of stakeholders. This is especially hard in the face of scarce resources, fragmented government, and the reality that many of the scenarios of large-area, long-duration outages are beyond the realm of experience of most individuals and governing systems.

<sup>6</sup> More than 10,000 MW means more load than that required to power all of New York City. In 2015, the summer coincident peak demand of Zone J (New York City) of the New York grid was 10,410 MW. The population of New York City's five boroughs is 8.5 million people, and the population of the New York City Metropolitan Statistical Area (which includes parts of New Jersey, Connecticut, and Pennsylvania) is more than 20 million. The New York City Metropolitan area accounts for roughly \$1.431 trillion in economic activity (NYISO, 2016; USCB, 2016; IHS Global Insight, 2013).

<sup>7</sup> The events that cause such large-scale outages cause damages to physical structures, including the electricity system, as well as impacts on economic activity. The costs of weather-related power outages are estimated to be billions of dollars annually, with estimates for Superstorm Sandy at \$14–26 billion (EOP, 2013). The potential long-term economic effect of such events in terms of losses and gains in economic activity and accounting for rebound is a more difficult estimate but clearly can be very large.

<sup>8</sup> Most of the damage from Sandy occurred after the winds had dropped below hurricane force and the storm had lost its tropical cyclone characteristics. Thus, the committee uses the term "Superstorm Sandy" and not "Hurricane Sandy" when it refers to this event.



**BOX 1.1****Examples of Outages on Bulk Power Systems and Their Consequences**

The five events summarized below exemplify the types of outages that can result from weather conditions, operational failures, or malicious hacking of the grid. (See Appendix E for a more comprehensive list and description of major outages in the United States.)

**New England/Eastern Canada Ice Storm (1998)**

Between January 4 and January 10, 1998, a series of storms generated along a stationary weather front brought warm Gulf of Mexico precipitation events across a stationary cold air mass (National Weather Service, 1998). While ice storms are common in Eastern Canada, this storm was unique for its long duration (more than 80 hours of freezing rain and drizzle), large geographical extent, and extraordinary freezing rain precipitation totals, with an accumulation of freezing rain greater than 3.1 in (80 mm) thick stretched from southeastern Ontario and northern New York State into southwestern Québec (RMS, 2008). The tremendous weight of accumulated ice resulted in the collapse of 770 electric transmission towers, the replacement of more than 26,000 distribution poles and 4,000 pole-top transformers, and the re-stringing of 1,800 miles of transmission and distribution circuits. At its peak, more than 5.2 million customers in the interconnected areas of Eastern Canada, New York, and New England were without power. Three weeks after the storm, hundreds of thousands of customers still had no power, with some customers not getting power restored until more than 1 month later (RMS, 2008). Storm damage was estimated to be approximately \$4 billion (National Weather Service, 1998).

**Northeast Blackout (2003)**

The August 2003 blackout is the single largest loss of power in U.S. history and was caused by a confluence of factors. A combination of software and operator errors occurring at the Cleveland utility (FirstEnergy) and at the regional reliability coordinator (Midwest Independent Transmission System Operator) greatly reduced the ability of the grid to withstand a reliability event. The regional system operator experienced diminished situational awareness, limiting its ability to intervene to assure system reliability. For example, loss of generation capacity in the Cleveland area adversely affected the ability of key transmission lines into the area to operate at a higher load than usual, but not enough to cause an equipment failure in and of itself. But other factors then triggered outages: contact with overgrown trees in transmission easements into Cleveland ended up tripping several 345 kV lines out of service, and FirstEnergy and Midwest Independent Transmission System Operator were unable to effectively monitor and respond to these losses of electric supply (NERC, 2004). The resulting power flows then redistributed from high-voltage system to lower-voltage lines, leading 16 lines to trip out of service in a 30-minute period, which ultimately caused a cascading collapse of the bulk power system across eight states and two Canadian provinces. The cascading failure left more than 50 million people without power. In certain parts of the outage area, power was not restored for 4 days. The blackout is estimated to have cost between \$4 billion and \$10 billion and contributed to 11 deaths (USCPSOTF, 2004).

**Hurricane Katrina (2005)**

Hurricane Katrina—the all-time most costly weather-related event in the United States—first hit land in Florida as a Category 1 storm, then grew to a Category 5 storm in the Gulf of Mexico before weakening to a strong Category 3 storm at second landfall, with severe storm surges along the Alabama, Mississippi, and Louisiana coastlines (NOAA, 2016). New Orleans experienced devastating flooding and widespread electricity outages, but ultimately damaging storm impacts were felt in eight states across the Southeast (NOAA, 2016). Katrina's impacts included loss of electric service to 2.7 million customers in these states; even 4 weeks after the storm, approximately 250,000 electric customers remained without service (DOE, 2009). In all, the storm destroyed 72,447 utility poles, 8,281 transformers, and 1,515 transmission structures; it took 300 substations off-line, and multiple power plants, including three nuclear plants, either shut down or had to reduce power (DOE, 2009). The flooding in New Orleans prevented full restoration of power for several months. At Southern Company's Mississippi Power, every customer lost power, "nearly two-thirds of the transmission and distribution system was damaged or destroyed, and all but three of the company's 122 transmission lines were out of service. . . . In the distribution system, about 65 percent of facilities were damaged. . . . Mississippi Power's second-largest electricity generating plant was damaged by floodwaters, which affected the company's emergency operations center and backup control center located in the plant. . . . Mississippi Power began tracking Katrina's progress, and 3 days before it hit Mississippi, Mississippi Power began making requests for manpower, material, and logistics. . . . Within 7 days after Katrina, 10,800 workers from 23 states and Canada were assisting Mississippi Power" (Ball, 2006). Katrina's estimated damage ranges from \$84.8 billion to \$157.5 billion (CBO, 2005).

**Superstorm Sandy (2012)**

In October 2012, Superstorm Sandy struck the eastern United States, impacting 24 states in its path. During the 7 days from Sandy's formation to its dissipation, the storm caused swells in excess of 3 meters, flooding in densely populated centers, and extensive damage to infrastructure, with a majority of the damage occurring in New York and New Jersey (FEMA, 2013). Considerable advance notice of the storm allowed electric utilities to make several preemptive steps to mitigate damages, including requests for more assistance from teams from other utility systems, for tree trimming along transmission lines, and for increased readiness of utility outage repair teams (EOP, 2013). It has been estimated that 8 million



customers lost power (Sandalow, 2012). Restoration services reported that 10 to 11 percent of customers in New York and New Jersey remained without power 10 days following the storm. During the outages, 50 deaths were attributed to the lack of electricity, with causes including hypothermia and improperly operated generators. The cost from the post-Sandy power outages has been estimated between \$14 billion and \$26 billion (EOP, 2013).

#### **Cyber Attack on Ukrainian Power Grid (2015)**

In December 2015, a synchronized multi-target cyber attack was executed on three electric grid control centers in eastern Ukraine (DHS, 2016; Volz, 2016). Months previously, the attackers had used “spear-phishing” tactics on employees via a Microsoft Office document to access the corporate networks (E-ISAC and SANS ICS, 2016). The attackers spent the following months learning about the system and its users to gain the necessary credentials to remotely access the communications networks (i.e., supervisory control and data acquisition systems) that control the operation of the electric grid. In December 2015, the attackers began the intrusion by shutting down power to the control center to prevent utility employees from effectively handling the outage (E-ISAC and SANS ICS, 2016). With that response capability compromised, the cyber attackers took control of the electric-system substations themselves and opened substation breakers to shut down power to a larger customer base. Simultaneously, the cyber attackers executed a “denial of service attack” on the customer support facilities, which made the related computer facilities unavailable to customers who sought to report outages and then released malicious software targeted at the master boot record. The attack left approximately 225,000 people without electricity for up to 6 hours. The release of malicious software wiped out personnel computers, servers, and remote terminal units (RTUs), which in turn delayed restoration of service and increased the amount of time required to bring control systems back online. Several substations suffered damage due to the attacks. Although NERC has classified the impacts of these attacks as low due to the short duration of the outage, the relatively small number of infrastructure affected, and the low population percentage of Ukraine that lost power (E-ISAC and SANS ICS, 2016), the attack nonetheless had far-reaching impacts. As of Fall 2016, the utility in Ukraine had yet to reach operational levels experienced prior to the attack, and it is currently unknown when the organization will reach peak operational capabilities again (E-ISAC and SANS ICS, 2016). Thus, in contrast to the other events described here, the Ukraine event was not a long-duration outage event for customers.

Some causes, like major solar coronal mass ejections (see Chapter 3), have very low probabilities of occurrence—sometimes measured in centuries. Others, such as cyber attacks, may become increasingly likely to impact the operations of the grid. Drawing on the tools of decision analysis, an analyst can help a unitary utility-maximizing actor determine how much to spend either to harden a system or to minimize the consequences of disruptive events. However, neither U.S. society, nor its power system, is governed by a single rational actor, but rather is collectively managed by many.

By design and of necessity in our constitutional democracy, making such decisions is an inherently political process. This committee of experts can identify risks and options, outline strategies to improve the understanding of relevant public and private decision makers, and suggest ways to assure that relevant factors are identified and considered. However, ultimately, the choice of how much resilience our society should and will buy must be a collective social judgment.

Large-area, long-duration outages are rare events. And investing in a more resilient system has the classic characteristics of “public goods” issues—localized and concentrated costs with broadly diffused and difficult-to-measure benefits—that are inherently difficult to address. It is unrealistic to expect firms to make voluntary investments whose benefits may not accrue to shareholders within the relevant

commercial lifetime for evaluating projects. Moreover, much of the benefit from avoiding such events, should they occur, will not accrue to the individual firms that invest in these capabilities. Rather, the benefits are diffused more broadly across multiple industries and society as a whole.

In some parts of the United States, rural electric cooperatives, vertically integrated utilities, and utility regulators may be better able to take a longer-term perspective that considers such broader societal benefits. But too often decision makers are pressed by short-term considerations of cost and choices about where expenditures should be directed for various and sometimes competing purposes, and so they must have a strong basis for approving expenses for activities that may not yield benefits for decades or longer. At the national level, the Federal Energy Regulatory Commission and NERC have the ability to adopt a somewhat longer-term perspective, although they too face short-term pressures and fiscal constraints.

No single entity is responsible for assuring the system is resilient in the face of all of them. Strategies to assure more systematic planning and to cover the costs of needed investments are discussed in Chapter 7. Many of the actions designed to reduce system vulnerability to one specific event can actually provide effective protection against a variety of events. For example, in regions where flooding is not an issue, undergrounding power lines can make the system less vulnerable to the impacts of severe storms as well as vehicle

## INTRODUCTION AND MOTIVATION

accidents. This may make such actions and investments easier to justify. Experience demonstrates the normal cycle of public reactions to major events with big impacts on society: there is a tendency not only to identify parties that can be blamed for failing to prevent the event and its impacts, but also to call for greater protective action against exactly the type of event just experienced. Regulators and other decision makers need to have well developed plans that can be implemented during such a “policy window” and designed for robustness against a wide range of threats.

There are some communities at considerably greater risk than others, including those at vulnerable locations in the electricity system or those within or close to natural hazards. When those communities take action, the results can serve as a stimulus and template for others to follow. Some modest government pilot funds to initiate such examples can be a socially prudent investment. At the same time, it is important that the United States devise ways to increase the likelihood that lessons learned from demonstrations can be diffused more widely. National organizations such as the National Association of Regulatory Utility Commissioners, the Edison Electric Institute, the National Rural Electric Cooperative Association, the American Public Power Association, and the National Governors Council can play important roles, raising awareness, sharing best practices, and providing guidance to members. Public and private partnerships such as the Electricity Subsector Coordinating Council, which gained importance following Superstorm Sandy, also serves as a viable forum for enhancing coordination and communication; conducting drills and exercises; and sharing tools and technologies to enhance grid resilience.

Throughout this report, the committee has tried to be attentive to the tension between two competing realities. One is that the electric power system and its regulation are decentralized across the many states and regions. The other is that a coherent strategy will not emerge without stewardship at the federal level and/or from organized leadership from public and private institutional partners that support actions in the national interest. The Department of Homeland Security (DHS) is specifically charged with identifying potential vulnerabilities and assisting in the development and implementation of strategies to reduce risks and increase resilience. However, neither DHS nor the set of local actors that typically interact with DHS control or run the power system. Moreover, the department is stretched very thin and has relatively modest technical expertise in the context of electric power systems.

As the energy sector lead agency and with its focus on research, DOE does have a longer-term perspective and hence is in a position to lay the groundwork and demonstrate the feasibility of a variety of technologies and strategies that, when adopted by others, can considerably enhance the resilience of the grid. Multiple DOE offices have programs related to electric power grid resilience. Specifically, the Office of Electricity Delivery and Energy Reliability and

Office of Energy Efficiency and Renewable Energy have responsibility for directing work on many of the nation's grid modernization and system integration programs and thus have a vital role to play in this area.

The Electric Power Research Institute can also make important contributions—including improving awareness of technologies and practices that are emerging globally—but the amount of fundamental longer-term work they can support is limited. The National Rural Electric Cooperative Association is undertaking a range of research activities that adopt a longer-term perspective. Many states around the country are also working on specific resilience projects, often in the aftermath of those states having experienced disruptive events that have focused policy makers' attention on the issue.

In the chapters that follow, the committee identifies and discusses many things that both the federal government and industry can do to advance the resilience of the power system. In Chapter 7, the committee returns to the broader issues of who is in charge, how electricity system operators, regulators, and society more broadly should choose what is worth doing, and how to pay for it.

## STRUCTURE OF THE REPORT

Chapter 2 describes the nation's electric system as it now exists and as it is integrating and adapting to new technologies and changing regulatory and market environments. This chapter provides context for the rest of the report by describing current conditions and factors affecting grid resilience and discussing how these systems might evolve over the coming decades (even if they are changing in unpredictable ways). Chapter 3 describes the many causes of grid failure: the range and types of threats that can, and at least in some cases definitely will, arise to disrupt the operations of the electric grid. Chapters 4 through 6 discuss ways that grid planners and operators, along with the rest of society, can prepare for and reduce the frequency and duration of disruptions (Chapter 4), manage and mitigate the consequences of outages as they occur (Chapter 5), and restore the system to normal operations as rapidly as possible (Chapter 6). These three chapters identify and discuss things already taking place, things that could improve the performance of each aspect of resilience, and things that deserve further attention from researchers and analysts; from owners, operators, and planners of the grid; and from government policy makers. Discussions of topics such as distributed energy resources and microgrids are spread throughout these chapters. Depending on how they are deployed, distributed energy resources and microgrids can be used for many purposes—they can help mitigate and prevent outages (Chapter 4), can help sustain electricity service to critical facilities during an outage (Chapter 5), and can aid in system restoration (Chapter 6). Throughout these chapters, as well as Chapters 2 and 3, the committee makes many specific recommendations

for strategies to increase the resilience of the U.S. electricity transmission and distribution system. While these specific recommendations will advance this purpose, the committee believes that the nation should adopt a more integrated perspective across the numerous, diverse institutions responsible for the resilience of the electricity system. Thus, the final chapter (Chapter 7) brings together a broader set of overarching recommendations intended to bring such an integrated perspective to the issue of electricity system resilience. The report Summary contains both the overarching recommendations and a synopsis of the chapter-specific recommendations.

## REFERENCES

- Ball, B. 2006. Rebuilding electrical infrastructure along the Gulf Coast: A case study. *The Bridge: Linking Engineering and Society*. Washington, D.C.: National Academy of Engineering.
- CBO (Congressional Budget Office). 2005. Macroeconomic and Budgetary Effects of Hurricanes Katrina and Rita. Testimony before the Committee on Budget. U.S. House of Representatives. October 6.
- DHS (Department of Homeland Security). 2016. "DHS Works with Critical Infrastructure Owners and Operators to Raise Awareness of Cyber Threats." <https://www.dhs.gov/blog/2016/03/07/dhs-works-critical-infrastructure-owners-and-operators-raise-awareness-cyber-threats>. Accessed February 27, 2017.
- DOE (Department of Energy). 2009. *Comparing the Impacts of the 2005 and 2008 Hurricanes on U.S. Energy Infrastructure*. <https://www.ee.netl.doe.gov/docs/HurricaneComp0508r2.pdf>.
- DOE. 2015. *Grid Modernization Multi-Year Program Plan*. <https://energy.gov/sites/prod/files/2016/01/f28/Grid%20Modernization%20Multi-Year%20Program%20Plan.pdf>.
- EIA (Energy Information Administration). 2000–2015. *Electric Power Monthly*, Table B.2. <https://www.eia.gov/electricity/monthly/backissues.html>. Accessed July 13, 2017.
- EIA. 2016. *Electric Power Annual*. <https://www.eia.gov/electricity/annual/>. Accessed July 13, 2017.
- E-ISAC (Electricity Information Sharing and Analysis Center) and SANS ICS (Industrial Control Systems). 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. [https://ics.sans.org/media/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_5.pdf](https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf).
- EOP (Executive Office of the President). 2013. *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*. [https://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report\\_FINAL.pdf](https://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf).
- FEMA (Federal Emergency Management Agency). 2013. *Hurricane Sandy FEMA After-Action Report*. [https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy\\_fema\\_aar.pdf](https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf).
- Flynn, S.E. 2008. America the resilient: Defying terrorism and mitigating natural disasters. *Foreign Affairs* 87: 2–8.
- GMLC (Grid Modernization Laboratory Consortium). 2016. "Foundational Metrics Analysis." <https://gridmod.labworks.org/projects/foundational-metrics-analysis>. Accessed February 27, 2017.
- IHS Global Insight. 2013. *U.S. Metro Economies*. <http://www.usmayors.org/metroeconomies/2013/201311-report.pdf>.
- National Weather Service. 1998. *Service Assessment: The Ice Storm and Flood of January 1998*. <http://www.weather.gov/media/publications/assessments/iceflood.pdf>.
- NERC (North American Electric Reliability Corporation). 2000–2009. *Event Analysis: System Disturbance Reports*. <http://www.nerc.com/palrrm/ea/System%20Disturbance%20Reports%20DL/Forms/AllItems.aspx>. Accessed July 13, 2017.
- NERC. 2004. *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* [http://www.nerc.com/docs/docs/blackout/NERC\\_Final\\_Blackout\\_Report\\_07\\_13\\_04.pdf](http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf).
- NERC. 2013. "Reliability Terminology." <http://www.nerc.com/AboutNERC/Documents/Terms%20AUG13.pdf>.
- NIAC (National Infrastructure Advisory Council). 2010. *A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations by the Council*. <https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf>.
- NOAA (National Oceanic and Atmospheric Administration). 2016. "U.S. Billion-Dollar Weather and Climate Disasters 1980–2016." <https://www.ncdc.noaa.gov/billions/events.pdf>.
- NRC (National Research Council). 2012. *Terrorism and the Electric Power Delivery System*. Washington, D.C.: The National Academies Press.
- NSF (National Science Foundation). 2016. "Cyber-Physical Systems." [https://www.nsf.gov/funding/pgm\\_summ.jsp?pims\\_id=503286](https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286). Accessed February 27, 2017.
- NYISO (New York Independent System Operator). 2016. *2016 Load & Capacity Data*. [http://www.nyiso.com/public/webdocs/markets\\_operations/services/planning/Documents\\_and\\_Resources/Planning\\_Data\\_and\\_Reference\\_Docs/Data\\_and\\_Reference\\_Docs/2016\\_Load\\_Capacity\\_Data\\_Report.pdf](http://www.nyiso.com/public/webdocs/markets_operations/services/planning/Documents_and_Resources/Planning_Data_and_Reference_Docs/Data_and_Reference_Docs/2016_Load_Capacity_Data_Report.pdf).
- Peifenberger, J.P., K. Spees, K. Carden, and N. Wintermante. 2013. *Resource Adequacy Requirements: Reliability and Economic Implications*. The Brattle Group, prepared for the Federal Energy Regulatory Commission. <https://www.ferc.gov/legal/staff-reports/2014/02-07-14-consultant-report.pdf>.
- RMS (Risk Management Solutions). 2008. *The 1998 Ice Storm: 10-Year Retrospective*. [http://forms2.rms.com/rs/729-DJX-565/images/wtr\\_1998\\_ice\\_storm\\_10\\_retrospective.pdf](http://forms2.rms.com/rs/729-DJX-565/images/wtr_1998_ice_storm_10_retrospective.pdf).
- Sandalow, D. 2012. "Hurricane Sandy and Our Energy Infrastructure." <https://energy.gov/articles/hurricane-sandy-and-our-energy-infrastructure>. Accessed February 27, 2017.
- USCB (U.S. Census Bureau). 2016. "Annual Estimates of the Resident Population: April 1, 2010 to July 1, 2015." <https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=bkmk>. Accessed February 27, 2017.
- USCPSOTF (U.S.-Canada Power System Outage Task Force). 2004. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. <https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>.
- Volz, D. 2016. "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage." *Reuters*, February 25.

## 2

## Today's Grid and the Evolving System of the Future

### INTRODUCTION

This chapter describes the U.S. electric system as it now exists and discusses how it may evolve over the next several decades. First, the committee provides background on the physical, ownership, legal/regulatory structure, and operational characteristics of the nation's electric system, with an emphasis on transmission and distribution infrastructure. The committee focuses on aspects of the national grid that are relevant for understanding electricity system resilience and the strategies employed to enhance it.<sup>1</sup> This overview of transmission and distribution also highlights the sensing, communications, and control systems that currently exist to support a variety of functions on the grid. Then, the committee describes the complex and dynamic forces driving changes in the electricity sector, both in the near term and the long term.<sup>2</sup> Finally, the committee discusses a variety of ways in which the system may change and some of the implications of these changes for the future resilience of the grid. Together, these conditions and trends set the stage for a subsequent discussion of threats to the system (in Chapter 3) and activities associated with each stage of resilience in the electric system (in Chapters 4 through 6).

Strategies to increase the resilience of today's transmission and distribution systems need to accommodate possible future changes in its character, because most of the physical assets and other pieces of the infrastructure have long lifetimes. Planning to enhance resilience should take this into account, along with the often uncertain ways these systems might evolve over the coming decades.

**Finding:** Approaches to assure resilience should consider that components of electricity infrastructure have long lifetimes and that how the grid and its various institutions,

technological features, legal structures, and economics will change is inherently uncertain.

### ELECTRIC INDUSTRY STRUCTURE, ASSET OWNERSHIP, AND OPERATIONAL ROLES AND RESPONSIBILITIES

Since the 1930s in the United States, most electric service to households, businesses, and other customers has been provided by investor-owned or publicly owned electric utilities responsible for all elements of electric supply: generation, transmission at high voltage, and local distribution of power at low voltage. That said, in the first half of the past century the federal government promoted electrification and developed hydropower resources aggressively. This led to the federal government operating several electricity generation and transmission organizations, perhaps the most famous of which are the Tennessee Valley Authority in the southeastern United States and the Bonneville Power Administration in the Pacific Northwest. Figure 2.1 depicts the “bulk energy system,”<sup>3</sup> comprised of central-station power plants and high-voltage transmission lines, and the local “distribution operations” that move power from the bulk system to end-use customers.

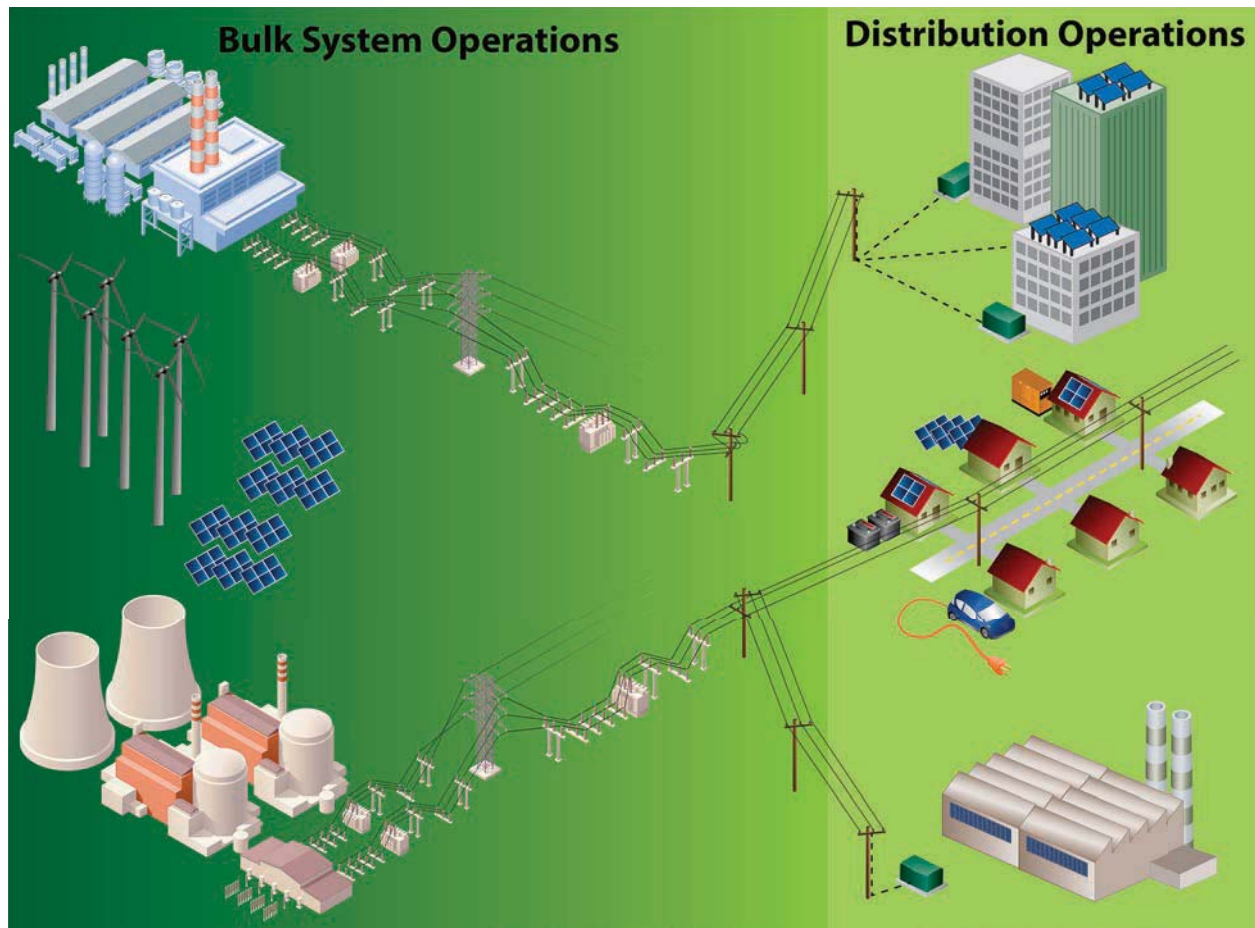
Several decades ago, most electric utilities were vertically integrated, meaning that the utility owned the power plants and/or contracts for power; owned or had rights to use high-voltage transmission lines that carry power from remote power plants to their local systems; and owned and operated the low-voltage distribution system to deliver power to consumers. State utility regulators (or, in the case of publicly

<sup>1</sup> Readers interested in a more detailed description might look at DOE (2017a), NASEM (2016), DOE (2015), MIT (2011), NRC (2012), and Bakke (2016).

<sup>2</sup> Readers interested in a more detailed description might look at MIT (2016).

<sup>3</sup> The Federal Energy Regulatory Commission has approved the following definition of “bulk energy system” as developed by The North American Electric Reliability Corporation: “All transmission elements operated at 100 kV or higher and real power and reactive power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electrical energy” (NERC, 2016a). There are specific technical exclusions of certain facilities from this definition, but the 100-kV dividing line between bulk energy system (and transmission-level voltage) and lower voltage (and distribution-system-level voltage) is useful for our purposes here.





**FIGURE 2.1** The bulk energy system encompasses the facilities and control systems for generation and transmission of electricity but does not include local distribution systems.

SOURCE: Courtesy of the Electric Power Research Institute. Graphic reproduced by permission from the Electric Power Research Institute from its research report, *The Integrated Grid: A Benefit-Cost Framework*. EPRI, Palo Alto, Calif: 2015. 3002004878.

owned utilities, the governing boards of the local utility) set rates for vertically integrated utilities based on the cost of providing service. But nearly 20 years ago, a number of states and federal regulators began to move aggressively to break up vertically integrated utilities, separating the ownership of generation, high-voltage transmission, and distribution systems. In those states, only the distribution part of the system has continued to operate as a regulated monopoly.

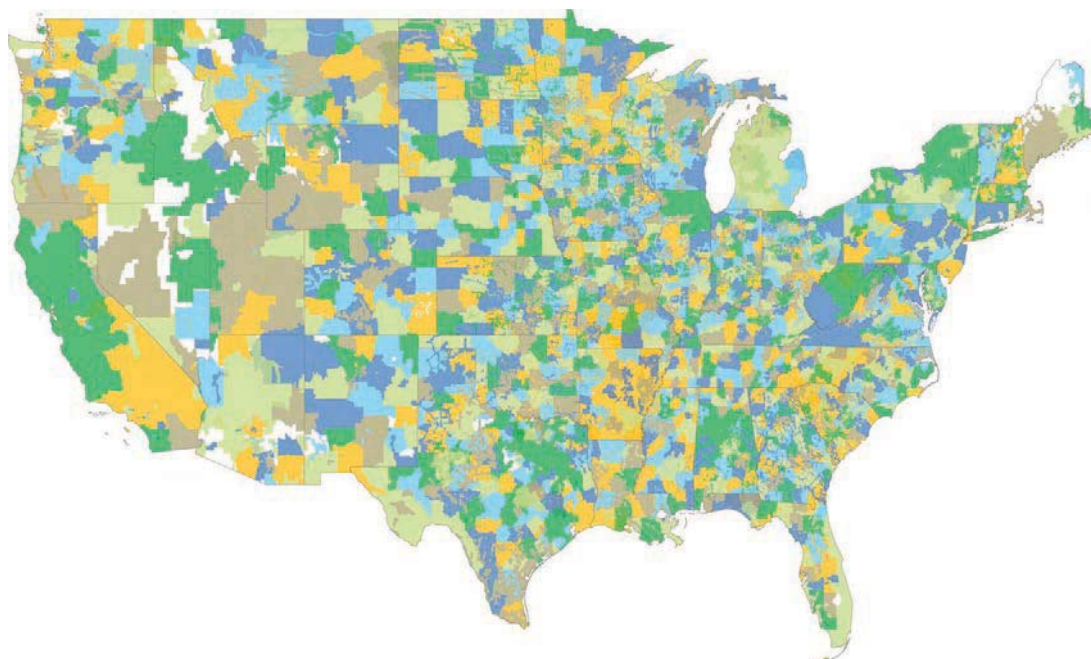
As the electric system developed over the decades, investor-owned electric utilities in many parts of the United States merged so as to provide power to customers over larger and larger service territories. In other parts of the country, utilities serve smaller numbers of customers, particularly in rural regions where local electric cooperatives and municipally owned utilities continue to be the dominant providers of electric service. The result is today's patchwork of local distribution utilities (Figure 2.2): thousands of electric utilities provide monopoly service within their local footprint but with a complex system of interconnected facilities that

operates, in effect, as a single "machine" within each interconnection (NAE, 2003).

According to the Energy Information Administration (EIA), there are more than 2,000 utilities that own and/or operate some part of the generation, transmission, or distribution infrastructure in the United States (Table 2.1). More than 70 percent of end-use electricity customers are served by just 174 large investor-owned utilities, while the remaining customers are split roughly evenly between publicly owned utilities and electric cooperatives. Although these investor-owned and publicly owned systems are physically connected, their transmission and distribution systems often have different configurations, voltage ranges, and technology demands; are owned and/or operated by different parties; are subject to different types of regulatory oversight; and are frequently discussed separately.

These many utilities operate as part of three separate interconnected "synchronous" regions within the United States (and parts of Canada), as shown in Figure 2.3. Within





**FIGURE 2.2** Map of electric distribution utility service territories in the continental United States.

SOURCE: Image reproduced with permission from Platts (2014), “Utility Service Areas of North America,” available for purchase online at <https://www.platts.com/products/utility-service-territories-north-america-map>.

each interconnection, the utility systems are physically tied together by major transmission lines. The 60 Hz voltage and current waveforms are synchronized across the entire region, and power flows within each region according to the laws of physics. The three interconnections operate with only a few (asynchronous) direct current (DC) connections that allow transfer of energy between them. The major transmission

lines serving the lower 48 states are shown in Figure 2.4. This figure also illustrates the strong synchronous connection with Canada for both the Eastern and Western interconnections, and the DC lines connecting the asynchronous Québec grid. The integrated North American power system mutually depends on close and continuing collaboration between the United States and Canada. And while there is also a connection to a small portion of Mexico within the Western Interconnection, that dependency is less significant for either country as most of the Mexican grid is a separate system.

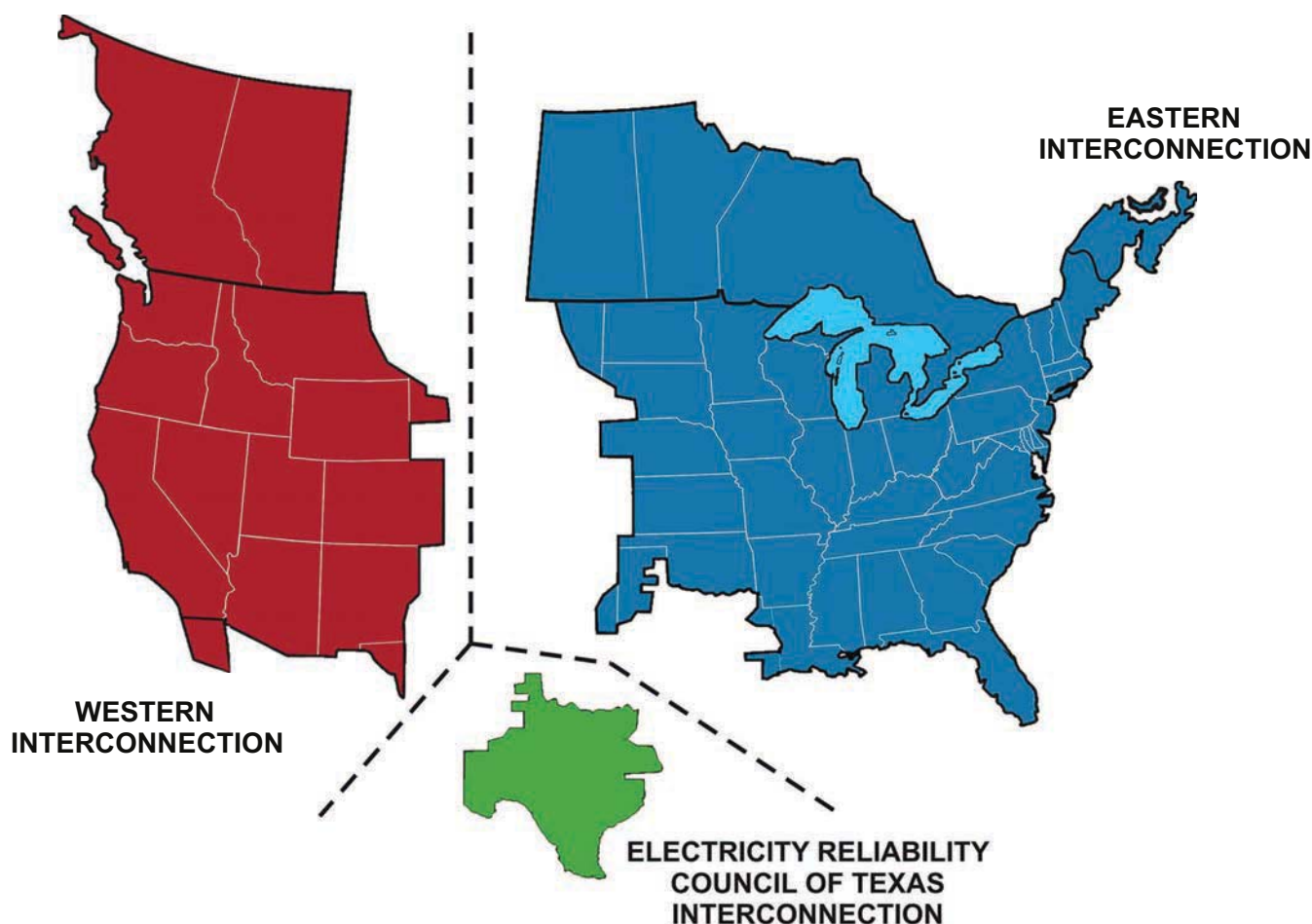
Regulation of the electric grid takes place at two levels. The operations, cost allocation, and cost-recovery of the interstate transmission system, as well as wholesale sales of electricity,<sup>4</sup> are largely regulated by the Federal Energy Regulatory Commission (FERC). FERC derives its authorities from the Federal Power Act (FPA), which was initially enacted in 1935 and has been amended multiple times. The second level of regulation occurs on distribution systems that deliver electricity to the end user. The terms and conditions of sales to retail electricity customers, including operations, cost allocation, and cost recovery for local transmission and distribution service, are subject to regulation by state regulatory agencies in those areas served by investor-owned

**TABLE 2.1** Breakdown of Utilities That Own and Operate Generation, Transmission, or Distribution Infrastructure

Utility Ownership Structure	Number
Rural electric cooperatives	809
Investor-owned	174
Municipally owned	827
Political subdivision	101
State power authorities	20
Federal utilities/Power marketing administrations	8
Other transmission companies	15
<b>TOTAL</b>	<b>1,954</b>

NOTE: Investor-owned utilities deliver 68 percent of electricity service to retail customers. Cooperatives, municipal utilities, and other publicly owned utilities deliver 13 percent, 12 percent, and 6 percent to retail customers, respectively. (As of 2015, 96 percent of electricity used by customers was sold through utility wires, with 4 percent generated on customers' own premises.) SOURCE: EIA (2016a).

<sup>4</sup> “Wholesale sales of electricity” are sales of power for resale to others, while “retail sales of electricity” are sales to ultimate, end-use customers. Retail sales are typically regulated by state utility regulatory agencies for investor-owned utilities (and by the governing entities of publicly owned or member-owned utilities).



**FIGURE 2.3** The three large electric interconnections that span the United States, large parts of Canada, and a small part of Mexico. A very modest amount of power flows among these three regions over direct current cables so that the 60 Hz power is not synchronized among the regions. Hydro Québec, which is not shown, provides power to many states in the northeastern United States.

SOURCE: DOE (2016a).

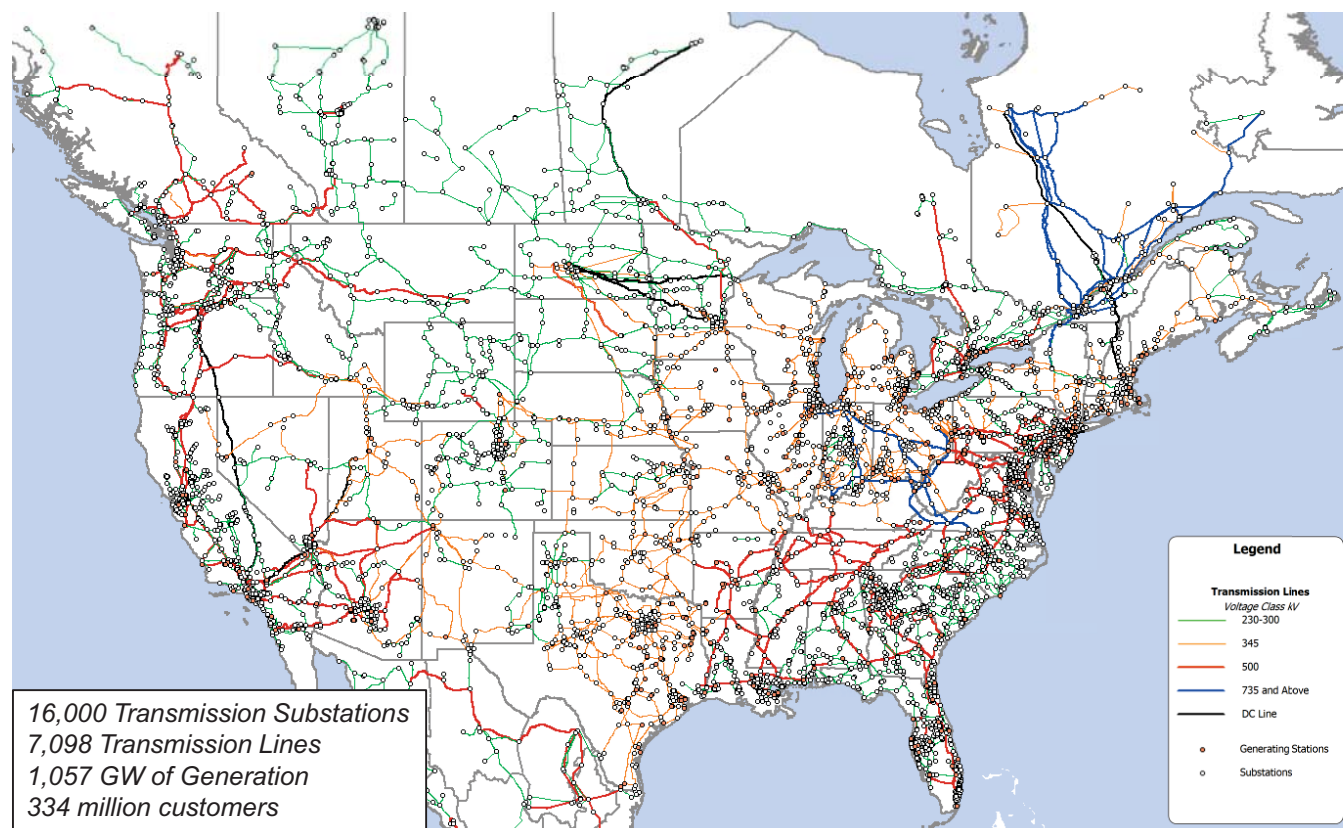
utilities and by publicly accountable boards of public utilities.

This regulatory division between the federal government and the states over the higher- and lower-voltage portions of the electric transmission system first appeared in its current form in the early 20th century and has largely remained in place since then.<sup>5</sup> Although seemingly straightforward, this division of authority is complex in practice and often gives rise to tensions. For example, although the FPA gives FERC authority over transmission service in interstate commerce and wholesale sales of electricity, the states have regulatory authority over siting of transmission lines (including the right to condemn right-of-way). Some states also retain regulatory authority over the costs of transmission as part of the bundled

delivery of retail electricity (in vertically integrated states as described later). Further, many states have the ability to adopt a variety of tax, siting, environmental, and other regulatory policies that affect the mix of power plants in a state.

More than 20 years ago, the electric industry began to undergo pressures for structural change, in part owing to the experiences of deregulating other commercial sectors such as airlines, interstate trucking, and telecommunications. Additional impetus came from federal policies that supported the introduction of relatively small-scale, economical generating technologies owned by non-utility companies, which led to requirements that utilities open up their transmission systems for use by third parties (e.g., the Public Utilities Regulatory Policies Act [PURPA] of 1978). Efforts began in a number of states in the mid-1990s to separate the ownership of generation assets from ownership of the transmission system (the “wires”) and to create competitive wholesale electricity markets. A primary motivation in doing this was a belief that introducing market forces into the industry

<sup>5</sup> As long-distance transmission lines emerged and utilities started to send power onto the grid across long distances, electricity began to cross state lines. Congress created FERC’s predecessor, the Federal Power Commission, in 1935 when it passed the Federal Power Act to address states’ inability to regulate interstate sales of electricity.



**FIGURE 2.4** The North American transmission system.

SOURCE: This information from the North American Electric Reliability Corporation's website is the property of the North American Electric Reliability Corporation and is available at <http://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/2015%20December%20Compiled%20Presentations.pdf>.

would result in lower costs to end users.<sup>6</sup> In fact, creation of competitive wholesale markets in many regions of the country required that non-discriminatory access to transmission infrastructure be provided to all generators. After an initial flurry of “restructuring,” some states began to have second thoughts and decided not to break up their vertically integrated utilities.

Today, there is a patchwork of restructured and vertically integrated utilities across the United States. In much of the country, there are hundreds of non-utility entities involved in the power generation, system operations, power marketing, power trading, and other affiliated activities. The market participants in the electric regions serving two-thirds of the population in the United States are members of organized wholesale electricity markets where a regional transmission organization (RTO) (sometimes called independent system operators [ISOs]) operates the transmission system, prepares regional transmission plans for the market footprint, and conducts competitive product markets (covering energy,

capacity, and/or ancillary services markets).<sup>7</sup> Figure 2.5 shows the boundaries of the current RTOs.

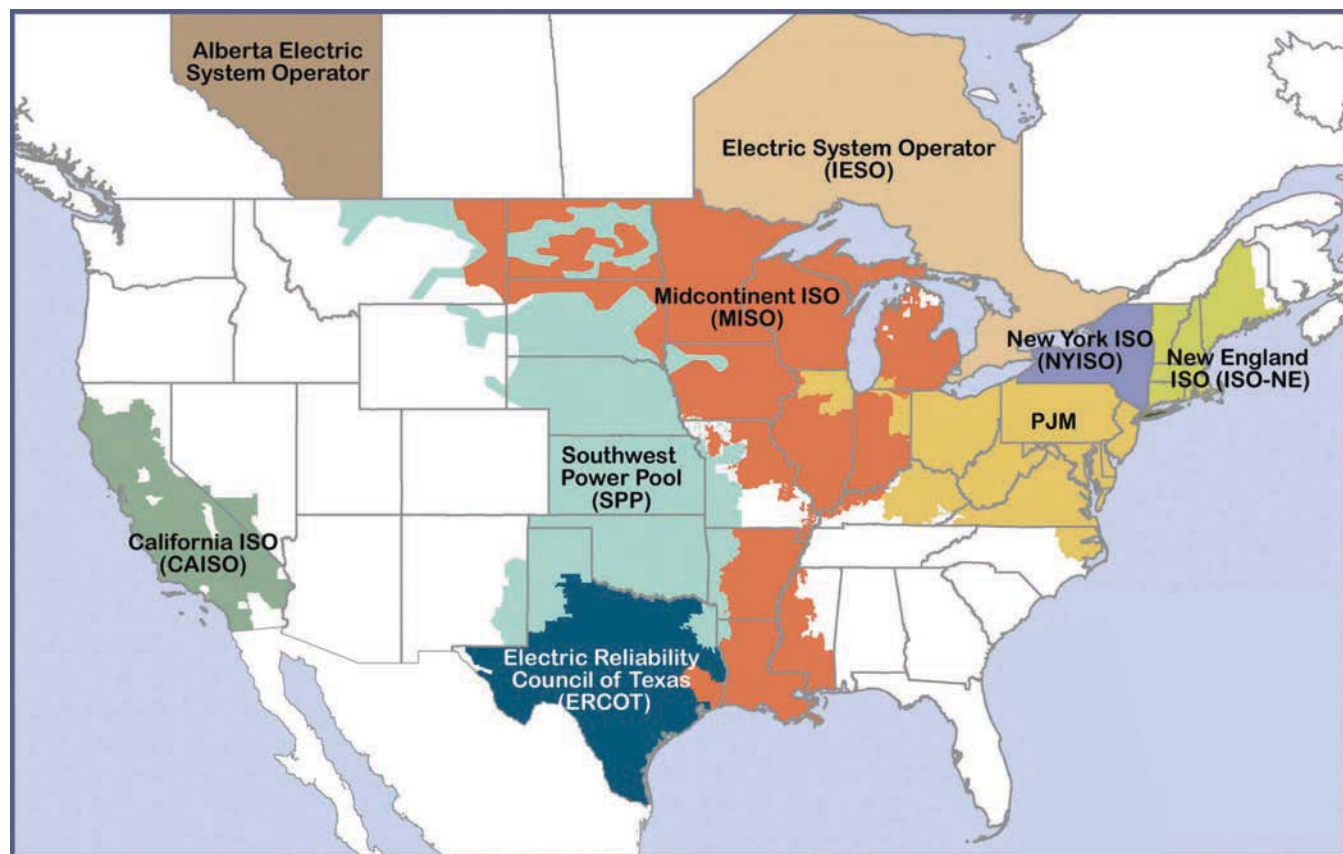
While retaining monopoly ownership of the distribution wires, several states also took steps to open up their electric systems to retail competition. In those shown in green in Figure 2.6, retail customers have the right to choose to buy electricity from competitive retail suppliers. Some states (shown in yellow) took initial steps toward allowing retail choice but then suspended it, while the remaining states (shown in white) did not introduce retail choice.

Across all of these areas, the specific terms and conditions of utility service, and any competitive supply, vary considerably. This makes it very difficult to generalize about industry structure across, and even within, states. At present this heterogeneous “electricity industry” reflects the varied choices that states and localities have made with regard to electric sector structure and regulation. The majority of states retain a vertically integrated structure, pursuant to which retail utilities maintain monopoly status with regard to the

<sup>6</sup> In fact, in most cases, rates did not decrease (Lave et al., 2004; Blumsack et al., 2008).

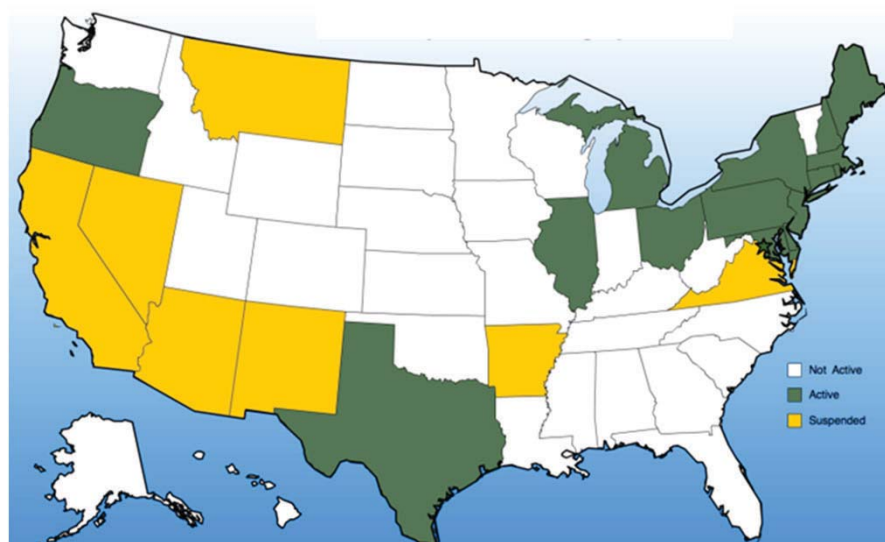
<sup>7</sup> As of 2015, these seven RTOs served 213.5 million, out of the total estimated U.S. population of 321 million (IRC, 2015; USCB, 2016).





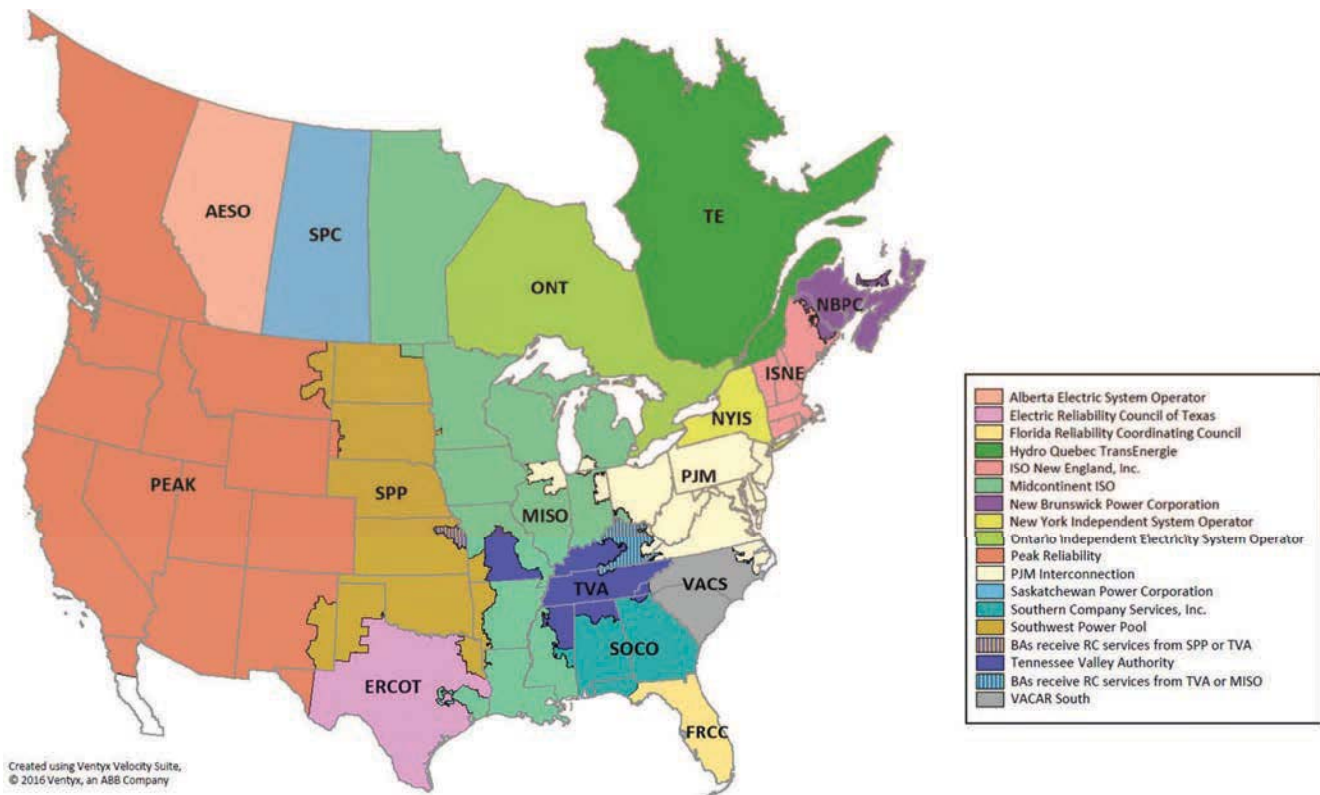
**FIGURE 2.5** Map of regional transmission organizations' (RTO) and independent system operators' (ISO) service areas in the United States and Canada. The parts of the country shown in white do not participate in an RTO, although as of this writing, several utilities in the western states have joined an "Energy Imbalance Market" administered by the California ISO.

SOURCE: FERC (2016a).



**FIGURE 2.6** End consumers can choose their electricity provider in restructured states (green), while other states have suspended restructuring activities (yellow) or never initiated them (white).

SOURCE: EIA (2010).



**FIGURE 2.7** North American Electric Reliability Corporation reliability coordinators are responsible for ensuring reliability across multiple utility service territories.

SOURCE: This information from the North American Electric Reliability Corporation's website is the property of the North American Electric Reliability Corporation and is available at <http://www.nerc.com/pa/rrm/TLR/Pages/Reliability-Coordinators.aspx>.

generation, sale, and delivery of electricity. Many states that have vertically integrated utilities without retail choice (e.g., California and many states in the Northern Plains and Upper Midwest) nonetheless have utilities participating in RTOs.

As shown in Figure 2.6, one-third of the states decided to introduce retail choice, and a majority of the states' utilities participate in the competitive generation markets administered by RTOs (shown in Figure 2.5), although the design of these markets varies across the seven RTOs.<sup>8</sup> In some states without retail choice—for example, in Colorado—non-utility companies may own rooftop solar panels that are physically located on a customer's building and sell that power to that customer. But, other such states without retail choice, such as Florida, do not allow anyone besides the utility to sell any form of electricity to consumers, although customers are able to install distributed generation on their premises. As a result of these variations across the states, the regulatory framework under which the electric grid operates takes on several forms. The FPA applies to the entire country but has differing impacts depending on which type of state-regional regulatory regime exists. This complicates

the landscape in which the resilience of the interconnected grid is implemented.

The ownership of transmission infrastructure also varies widely across the United States. In some regions, vertically integrated utilities and large public power providers such as the Bonneville Power Administration and the Tennessee Valley Authority both own and operate the transmission infrastructure. In regions with competitive power markets, operation of the transmission system is delegated to RTOs/ISOs. These organizations may not own the transmission infrastructure under their control, but they are responsible for meeting reliability standards and conducting regional planning efforts, while assuring non-discriminatory access to transmission services for all generators and load-serving entities in the region.

With respect to reliability issues, FERC has responsibility for assuring adherence to mandatory reliability standards for the electric industry. FERC has delegated responsibility for developing reliability standards to the North American Electric Reliability Corporation (NERC), which had originally formed as a voluntary reliability organization following a large blackout in 1965 and is now the designated reliability organization in the United States. NERC develops industry-wide standards, submits them to FERC for approval, and

<sup>8</sup> The only states that do not have any utilities participating in an RTO are Alabama, Alaska, Arizona, Colorado, Florida, Georgia, Hawaii, Idaho, Oregon, South Carolina, Utah, and Washington.



enforces approved standards in the industry. Thus, FERC does not develop reliability standards on its own. Compliance with NERC standards became mandatory with the passage of the 2005 Energy Policy Act (EPAct), and utilities and system operators now face substantial penalties for non-compliance.

Among many other things, NERC has defined the essential system functions necessary to ensure reliability in a framework that accommodates operational and structural differences across regions with and without competitive wholesale markets (NERC, 2010). Within each large region, there is a reliability coordinator with a wide-area perspective on system conditions necessary to ensure that the actions undertaken by one entity do not compromise reliability in another. Currently there are 12 reliability coordinators covering the Continental United States, much of Canada, and a small part of Mexico (Figure 2.7).

Under the purview of these reliability coordinators, more than 100 “balancing authorities” have responsibility for keeping generation and load equal at all times within smaller balancing areas. Regions with a history of tight coordination of operations and planning across utilities within the region, such as New England, New York, and the Mid-Atlantic

region (e.g., Pennsylvania, New Jersey, and Maryland, the original location of the PJM territory), have only a single balancing authority, whereas the majority of reliability coordinators interact with multiple balancing authorities within their footprint. Box 2.1 has examples of transmission system oversight and operation that vary by region.

NERC directs several industry working groups and activities related to preparing for, riding through, and recovering from events with high impacts on the bulk power system. In addition, the Electricity Subsector Coordinating Council (ESCC), formed in response to recommendations from the National Infrastructure Advisory Council, provides a high-level forum for utility executives and federal decision makers to engage and maintain open communication channels in preparation for large-scale outages. To help reduce risks of cyber and physical attacks, for example, NERC operates the Electricity Information Sharing and Analysis Center (E-ISAC), which disseminates information and alerts to electric industry and government representatives, conducts training exercises, and also maintains the Cyber Risk Information Sharing Program that covers nearly 80 percent of operators of the bulk power system. Through the Spare Equipment Working Group, NERC maintains a database of

### BOX 2.1

#### Examples of Four Different Electric Operational/Reliability/Ownership Structures

**Southern Company** (SoCo) is a large vertically integrated utility operating in several Southeastern states. SoCo owns generation assets with a total capacity over 44,000 MW, transmission lines, and four subsidiary distribution utilities. SoCo's electric utilities collectively serve a population of approximately 9 million people (SoCo, 2017). Through these four subsidiaries, SoCo serves the functions of transmission owner, distribution provider, and generation owner while another subsidiary, Southern Company Services, serves as the reliability coordinator, transmission operator, and balancing authority.

**PJM** is an RTO serving all or part of 13 states and the District of Columbia, ranging from Pennsylvania and New Jersey in the East, southward to Virginia, and westward to northern Illinois. PJM provides service in a region with approximately 61 million people and 171,000 MW of generating capacity (PJM, 2017). PJM serves as reliability coordinator, transmission operator, and balancing authority, while also administering the organized competitive wholesale electricity market. However, PJM is not a market participant per se, as other entities own the physical assets associated with generation, transmission, distribution, and power marketing.

**Bonneville Power Administration** (BPA) is a federally operated power marketing administration in the Pacific Northwest, which markets electricity generated from hydroelectric dams owned and operated by the U.S. Army Corps of Engineers or the Bureau of Reclamation (approximately 22,500 MW of capacity), a nuclear power plant, and other renewable generation assets operated by Energy Northwest. BPA's service territory includes Oregon, Washington, western Montana, and small parts of northern California, Nevada, Utah, and Wyoming. BPA owns and operates more than 15,000 circuit miles of transmission (BPA, 2017) and acts as a balancing authority that reports to the regional reliability coordinator. BPA does not own generation or distribution assets.

**Arizona Public Services** (APS) is a vertically integrated utility that owns and operates generation, transmission, and distribution assets. APS provides power to 1.2 million customers in 11 counties in Arizona and generates more than 6,100 MW of capacity (Hoovers, 2017). APS is a balancing authority that reports to the regional reliability coordinator, and, as of the last quarter of 2016, is participating in the Western-states' Energy Imbalance Market administered by the California Independent System Operator (CAISO).

system components, particularly large transformers, which are available to participating utilities should their assets be physically damaged (NERC, 2011). Similar programs are maintained by industry trade organizations, such as the Edison Electric Institute's (EEI) Spare Transformer Exchange Program and the Grid Assurance™ initiative recently launched by the private sector. Parfomak (2014) has prepared an excellent review of the issue of spare transformers for the Congressional Research Service. This report makes it clear that, while the past few years have seen progress, there is still much that needs to be done. The committee returns to the issue of replacement transformers in Chapter 6.

For many years, electric utilities have widely employed mutual-assistance agreements at both the transmission and distribution level to facilitate sharing of skilled workers and equipment to speed restoration efforts following outages. Typically restoration teams are composed with at least one local utility worker so that system-specific and regional knowledge is available on every team. After Superstorm Sandy, EEI developed a National Response Event Framework for pooling resources and coordinating restoration at the nation-scale from outages that overwhelm regional resources (discussed further in Chapter 6).

Thus, a hallmark of the U.S. electric system is that there are a myriad of bodies engaged in the ownership, planning, operation, and regulation of different elements of the system. Although the system itself operates as if it were a unified and coordinated machine, that occurs in spite of—or in the context of—a system in which the many component parts are subject to varied sets of institutional, legal, cultural, and financial incentives and penalties. Asset owners and operators must, and do tend to, operate with awareness of the fact that their systems can be impacted by events and developments occurring on other parts of the machine.

**Finding:** The “electric industry” is different across different parts of the United States in ways that reflect the varied choices that states and localities have made with regard to electric sector structure, asset ownership, and regulation. The specific terms and conditions of utility service, power system planning and operations, and transmission planning vary considerably, making it difficult to generalize about industry structure across and within the states. This complicates the landscape in which the issue of resilience of the interconnected grid must be addressed.

## PHYSICAL STRUCTURE AND OPERATION OF THE HIGH-VOLTAGE TRANSMISSION SYSTEMS

### Physical Structure

Most of the electricity supplied to today's bulk power system is generated by large, central generating stations, often located far from population centers. Roughly one-third of the U.S. electricity supply comes from power plants that

use natural gas, and another one-third comes from coal-fired generation. This reflects a significant increase in gas-fired generation in recent years, up from just 10 percent in 1990 (Tierney, 2016a). The fraction being generated by coal plants has fallen in large part because of competition from low-cost natural gas. Slightly less than 20 percent of generation comes from large nuclear plants. This share has been shrinking slowly, again because of competition from low-cost natural gas (and, to a lesser degree, flat demand and entry of renewable energy technologies) and the high cost of nuclear plant life extension. Hydropower produces 6 percent of the total U.S. power supply, with other renewables accounting for 7 percent of supply—most of that coming from wind (EIA, 2015). While power provided by large-scale wind and solar projects and from equipment such as solar panels located on customers' premises is rapidly growing, it still constitutes a relatively small share of the total supply. These national averages do not reflect that some systems, such as those in California and Hawaii, have much higher percentages of distributed generation and intermittent renewables.

Hundreds of thousands of miles of transmission lines operate in interconnected networks across the United States, which carry alternating current (AC) electricity. Example voltages include 115, 230, 345, 500, and occasionally 765 kV. A few long-distance point-to-point lines use high-voltage direct current (DC) transmission.<sup>9</sup> Electricity moves through the transmission system following the laws of physics and typically cannot be controlled precisely without expensive equipment.<sup>10</sup> The bulk power system relies on large step-up transformers to convert electricity generated at central generating stations to high voltages; this allows for more efficient transmission of power across long distances because there are lower resistive losses of power at higher voltages.

Within the three U.S. bulk-power transmission interconnections, generators operate synchronously at 60 Hz. Large-scale electricity storage is relatively rare;<sup>11</sup> thus, power production and consumption must be kept in balance near instantaneously by increasing or decreasing electricity generation to match changing demand as customers increase and decrease their electricity use. In some areas, in addition to changing the amount of power being generated, grid operators use demand response (DR) programs and technologies to reduce certain loads in lieu of providing more generation. Maintaining the stability of this complex and dynamic

<sup>9</sup> Direct current transmission is used selectively in the United States as a way to transfer power between asynchronous interconnects, occasionally to transfer bulk power over long distances (e.g., from the Pacific Northwest to California and from Labrador to the Northeast United States), and for underwater transmission (e.g., between Connecticut and Long Island and from offshore wind farms).

<sup>10</sup> Technologies that allow control of AC power flows include phase-shifting transformers and other emerging power electronics-based flexible AC transmission system devices that are becoming more available and giving operators more control than ever.

<sup>11</sup> At present, the primary form of large-scale storage capability resides in hydroelectric pumped-storage facilities.

interconnected electric system is an immense operational and technical challenge. Nonetheless, this balancing act is successfully accomplished around-the-clock throughout the grid but not without the complex array of tools, techniques, systems, and equipment dedicated to the task.

The high-voltage transmission network enables power to travel long distances from generating units to substations closer to local end-use customers where the voltage is stepped back down and sent into the distribution system for delivery to consumers. Many of the approximately 15,000 substations have minimal physical protection, exposing them to natural hazards, vandalism, and physical attacks (NERC, 2014). Given that there is no standard design for substations, and especially for the transformers they contain, repairs and replacements of custom-designed facilities can be costly and take many months or even years to complete.

Most power outages occur on the local distribution system. Outages are less frequent on the transmission system. However, when outage events happen on the transmission system, they tend to result in wider impacts and can impose greater costs. Several of the largest outages—introduced in Box 1.1 and listed in greater detail in Appendix E—have resulted from operational or control-system errors followed by equipment tripping off-line due to close proximity with vegetation, as was the case with the 2003 blackout. Given the underlying network configuration of the high-voltage grid, system imbalances caused by events in one place can propagate across the transmission system near instantaneously, with the risk of causing cascading blackouts that impact customers hundreds of miles from the site of the initial disturbance.

**Finding:** Given the interconnected configuration of the high-voltage grid, events in one place can propagate across the transmission system in seconds or a few minutes, potentially causing cascading blackouts that can affect customers hundreds of miles from the initial disturbance. Thus, outage events on the transmission system can result in large-area impacts.

### Sensing, Communication, and Control in the Transmission System

If electricity generation and consumption are not kept in balance, frequency will begin to rise or fall depending on whether there is a surplus or deficit of generated power, respectively. Deviations of voltage or frequency outside of relatively narrow boundaries can lead to physical damage to equipment and can increase the probability of a large-area cascading blackout. System operators depend upon various communications and other systems—for example, supervisory control and data acquisition (SCADA) systems in conjunction with software-based energy management systems (EMS)—to monitor the operating status (or state) of the transmission network and to control specific grid

components to maintain stability. These systems rely on various sensors located primarily at substations (and, to a lesser extent, on transmission lines) to collect and transmit a wide variety of data, including voltage and current characteristics at specific geographic locations; environmental variables such as temperature, wind speed, and ice formation; and measures of asset health such as transformer oil temperature and dissolved gas levels (PNNL, 2015).

Autonomous local controls (called “governors”) at individual generators that boost power output proportional to declining system frequency (and vice versa) are fundamental components of system control responsible for regulating system frequency. The rotational inertia provided by spinning generators and some loads in each interconnection determines the rate of frequency change. On a slower time scale, the 60 Hz frequency is regulated by each balancing authority re-dispatching generation every few seconds through a wide area control scheme called automatic generation control.

Protective relays on the transmission network locate, isolate, and clear faults by triggering the appropriate circuit breakers to disconnect at-risk parts before the system becomes unstable and damage results. Depending upon their vintage, protective relays may be electromechanical (the oldest), solid state, or programmable and microprocessor based. They can act and take effect within tens or hundreds of milliseconds. To maintain acceptable voltage across long distance transmission lines, devices such as capacitor banks and static volt-amp reactive<sup>12</sup> compensators are used to control voltage.

A complex system of communications infrastructure is essential to the reliable operational performance of the electric grid, and this dependence is growing. There is, however, wide variation in the sophistication and speed of communication technologies used across the nation's varied electricity systems, with equipment ranging from twisted wire, to wireless, to rented telephone line, to fiber-optic cable dedicated for utility use. The control of electricity systems is inherently challenging both because changes in the electricity system can occur very rapidly and because control needs to operate over time scales that range from milliseconds to multiple days.

To help system operators maintain system reliability, power systems have sensors, communications, and software that automatically perform analyses so as to constantly monitor the state of the electric system. The overall monitoring and control systems for transmission networks include displays and limit checking of all measurements for operators. A principal tool known as the State Estimator filters the various measurements and estimates the operational characteristics of the power system at regular intervals (e.g.,

<sup>12</sup> Delivered power is the product of voltage and current. In AC systems, only that portion of the current waveform that is in phase with the voltage waveform produces power. However, the out-of-phase current does flow in the lines and causes losses, so utilities strive to keep voltage and current waveforms in phase as close as possible.

every 30 seconds, although the time period used to be longer and continues to get shorter). This helps provide real-time assessments of system conditions that might not otherwise be observable by operators and improves their situational awareness. These assessments also enable other real-time analytic tools that can alert the operator to possible contingencies that could endanger the reliable operation of the grid.

Maintaining the security of these communication networks is critical to the operational integrity of the electricity system. Conversely, the integrity of these other systems (e.g., the internet and communications technologies) depends upon the operational integrity of the electricity system. Conventional approaches to cybersecurity such as firewalls, security software, and “air gaps” (i.e., no connection between systems) are used by utilities to protect their systems from intrusion. However, such measures are being recognized as inadequate, and the growing likelihood that breaches will happen motivates increased emphasis on cyber resilience, including intrusion detection and post-breach restoration. The importance of such activities is illustrated by the 2016 cyber attack on Ukraine’s electricity infrastructure. It took grid operators many months to even recognize that their systems had been compromised, at which point it was too late to prevent substantial outages from occurring.

To date, NERC has mandated nine cybersecurity standards as part of the overall mandatory standards it has established for the electric industry. These critical infrastructure protection (CIP) standards address the security of cyber assets essential to grid reliability.<sup>13</sup> In addition to the cybersecurity standards from the Nuclear Regulatory Commission, these are the only mandatory cybersecurity standards for any of the critical infrastructure sectors across the United States (NERC, 2017).

**Finding:** System operators depend upon SCADA systems in conjunction with software-based EMS to monitor the operating status of the transmission network and to control specific grid components to assure safe and reliable operation. Control is inherently challenging because it must operate over time scales that range from milliseconds to multiple days. Maintaining the security of power system communication

networks and control systems is critical to the operational integrity of the electric system.

**Finding:** CIP standards dictate minimum cybersecurity protections for the bulk power system, and the electricity sector is the only critical infrastructure sector with mandatory standards. However, these standards do not apply to local distribution systems.

## PHYSICAL STRUCTURE AND OPERATION OF THE DISTRIBUTION SYSTEM

### Physical Structure

The electric distribution system moves power from the bulk energy system to the meters of electricity customers. Typically, power is delivered to distribution substations from two or more transmission lines, where it is converted to a lower voltage and sent to customers over distribution feeders. Although distribution system outages tend to be more frequent than those occurring on transmission facilities, the impacts of such outages are smaller in scale and generally easier to repair.

Most local distribution systems in the United States are physically configured as “radial” systems, with their physical layout resembling the trunks and branches of a tree. Customers on radial systems are exposed to interruption when their feeder (i.e., their branch) experiences an outage. In metropolitan areas, these trunks and branches typically have switches that can be reconfigured to support restoration from an outage or regular maintenance. When a component fails in these systems, customers on unaffected sections of the feeder are switched manually or automatically to an adjacent, functioning circuit. However, this still exposes critical services such as hospitals or police stations to potential outages, so these facilities are often connected to a second feeder for redundancy. In high-density urban centers, distribution systems are often configured as “mesh networks,” with a system of interconnected circuits and low-voltage equipment able to provide high reliability service to commercial and high-density residential buildings. Such mesh networks—found in Manhattan, parts of Chicago and San Francisco, and other high-density urban areas—provide multiple pathways through which electric service may be provided to customers.

Most distribution systems’ wires are located above-ground. However, areas with high population density, including some suburban areas, frequently locate electricity and other infrastructure underground. This provides some physical protection and reduces risks posed by vegetation, but it can make identifying faults and implementing repairs more difficult and increase the risk of equipment damage in earthquake and flood-prone locations. In less densely populated areas, distribution feeders are usually located aboveground, with smaller distribution transformers located on local utility

<sup>13</sup> NERC has nine mandatory CIP standards related to cyber issues. These cover such things as reporting of sabotage (CIP-001); identification and documentation of the critical cyber assets associated with critical assets that support reliable operation of the bulk power system (CIP-002); minimum security management controls to protect critical cyber assets (CIP-003); personnel risk assessment, training, and security awareness for personnel with access to critical cyber assets (CIP-004); identification and protection of the electronic security perimeters inside which all critical cyber assets reside, as well as all access points on the perimeter (CIP-005); a physical security program for the protection of critical cyber assets (CIP-006); methods, processes, and procedures for securing critical cyber assets and other cyber assets within the electronic security perimeters (CIP-007); identification, classification, response, and reporting of cybersecurity incidents related to critical cyber assets (CIP-008); and recovery plans for critical cyber assets, relying upon established business continuity and disaster recovery techniques and practices (CIP-009) (NERC, 2017).



poles that step down to lower voltage for delivery to customers' premises.

There is no single organization responsible for establishing or enforcing mandatory reliability standards in distribution systems, although state utility regulators and boards of publicly or customer-owned utilities often assess performance using quantitative reliability metrics and set goals for the allowable frequency and duration of system and customer outages. Typically, utilities collect data on the length and frequency of outages that result from events on the local distribution systems, and some utilities (particularly investor-owned utilities with encouragement from regulators) disclose this information to the public. However, there is wide variation across the states and the utilities within them with regard to their tracking, publication, and/or enforcement of local reliability indicators. In light of their role in approving rates and in deciding what costs and other investments can be recovered through rates, public utility commissions (and boards of publicly or customer-owned distribution utilities) have significant influence on the reliability, cost, and resilience of distribution systems, as FERC does at the bulk energy system level.

In recent years in some parts of the United States, distribution systems have also experienced substantial additions of distributed energy resources (DERs). DERs are electrical resources that are attached to the local distribution system, often behind a customer's meter. Examples include rooftop solar panels, customer-owned batteries, fuel cell technologies, wind turbines, backup generators, and combined heat and power (CHP) systems.<sup>14</sup> Although DERs account for a relatively small fraction of total generation nationally, their installation varies significantly from one state to another, with some local distribution systems (e.g., in Hawaii, California, New Jersey, and Arizona) seeing hundreds of MW of growth in installed capacity in recent years (DOE, 2017a). Because many DERs provide surplus power beyond the amount of electricity consumed on the customer's premises, they inject power into a distribution system designed to operate in a one-way flow of power from the substation to the customer. (See "Near-Term Drivers of Change and Associated Challenges and Opportunities for Resilience" for a longer discussion of DERs and their implications for grid planning, operation, and resilience.)

Even with increasing numbers of consumers installing generating equipment on their own premises, and using the distribution system to access the bulk energy system when on-site generation is not available, it is unlikely that the majority will go entirely "off grid" in the near future. Although many technologies and service offerings are enabling an increasing number of customers to meet larger

portions of their electricity needs with on-site generation, for economic, technical, and regulatory reasons most observers (and the committee) do not anticipate that the dominant customer profile will be self-sufficient and disconnected from the grid during the time frame of interest in this study (i.e., in the next two decades). Moreover, individual self-sufficiency is unfeasible for the majority of the population, and local distribution system planners have to plan to meet the uncertain loads of customers for the foreseeable future.

**Finding:** There is no single organization responsible for mandatory reliability standards in electric distribution systems in the United States. State utility regulators often set standards for the allowable frequency and duration of system and customer outages. In many cases, outages caused by major events are *excluded* when computing reliability metrics.

### Sensing, Communication, and Control in the Distribution System

The technological sophistication, penetration of sensors, deployment of advanced protection devices, communications technologies, computing, and level of automation deployed by distribution utilities vary significantly across the United States. As in the case of transmission systems, distribution networks have been undergoing a transition from analog devices to digital. However, in many distribution systems, it is more difficult to justify large investments in modernization and digital controls, in part owing to factors such as customer density on circuits, circuit configurations, existing performance, and component age. Thus, many distribution systems still operate as they did when built after World War II. However, given the substantial investments (exceeding \$25 billion annually [EEI, 2017]) under way in replacing aging distribution infrastructure, there is an opportunity to enhance the reliability and resilience of the distribution systems through incorporation of advanced technologies, and some distribution utilities have made extensive upgrades.

Protective relays located at distribution substations are used to sense faults, such as a downed wire, and in turn signal the feeder circuit breaker to open. Some feeders have switches that can detect and isolate faults, albeit less frequently (as discussed previously). Distribution laterals that extend from the main feeders have fuses installed that protect the main feeder from faults that occur on the lateral branch. Together, protection devices are critically important for maintaining public safety and for limiting the extent of an outage, in some cases preventing disturbances from cascading higher up in the system.

Each of these devices, relays, switches, and fuses are designed to operate in a coordinated manner. These distribution protection schemes are undergoing a similar analog to the digital transformation occurring on transmission systems. Over the past 20 years, electromechanical relays

<sup>14</sup> Certain energy efficiency measures can function as DERs so long as they are dispatchable, meaning they can be turned on or off when needed by the utility. Other definitions do not emphasize that DERs be dispatchable—for example, FERC's definition at <https://www.ferc.gov/whats-new/comm-meet/2016/111716/E-1.pdf>.



have increasingly been replaced with digital, and now communicating, software-based relays as old equipment reaches end-of-life or when new substations are constructed. Similarly, switches on some feeders have been replaced with more advanced and automated switches when it is cost-effective and justifiable. Protective fuses also have digital communicating alternatives, but these are still largely in demonstration studies to evaluate cost-effectiveness and applicability.

Beginning in the 1990s, many utilities selectively installed SCADA on distribution systems for feeder breakers, mid-point reclosers, and back-tie switches (as well as capacitor bank controls), along with distribution management systems to operate these devices. These first-generation automation systems allowed utilities to operate circuit breakers, switches, and components remotely, which previously required personnel in the field. By sectionalizing circuits in half, these early systems allowed more rapid restoration of the faulted half of the circuit. Such systems have been implemented by many utilities in metropolitan areas where high customer densities enable cost-effective applications.

More recently, a second generation of distribution automation technologies has been adopted. Outage management systems (OMS) that provide greater visibility into distribution circuits and support operators in making restoration decisions have been deployed over the past decade. Some utilities have implemented advanced automation technologies that locate faults, isolate faulted sections, and automatically restore remaining sections to service. Similar to first-generation automation systems, these systems are typically cost-effective only in areas with high customer density per mile of line and on overhead lines with exposure to environmental conditions that reduce reliability and impair restoration.

Although at present these technologies have only been implemented on a fraction of distribution systems across the country, continued deployment of distribution substation SCADA and first- or second-generation automation has the potential to improve the reliability and resilience of the nation's distribution systems, albeit if implemented selectively and as part of a long-term improvement plan. For example, select utilities in areas with significant exposure to environmental threats (e.g., Southern Company in the southeastern United States), or with the need to have greater visibility and control over DERs (e.g., Southern California Edison), have installed or are pursuing advanced automation technologies for automatic reconfiguration of feeders based on outage and load/local generation conditions. However, it is unlikely that these second-generation automation technologies will be deployed in lower-density rural areas or in newer underground systems, as the potential benefits do not typically justify the increased costs.

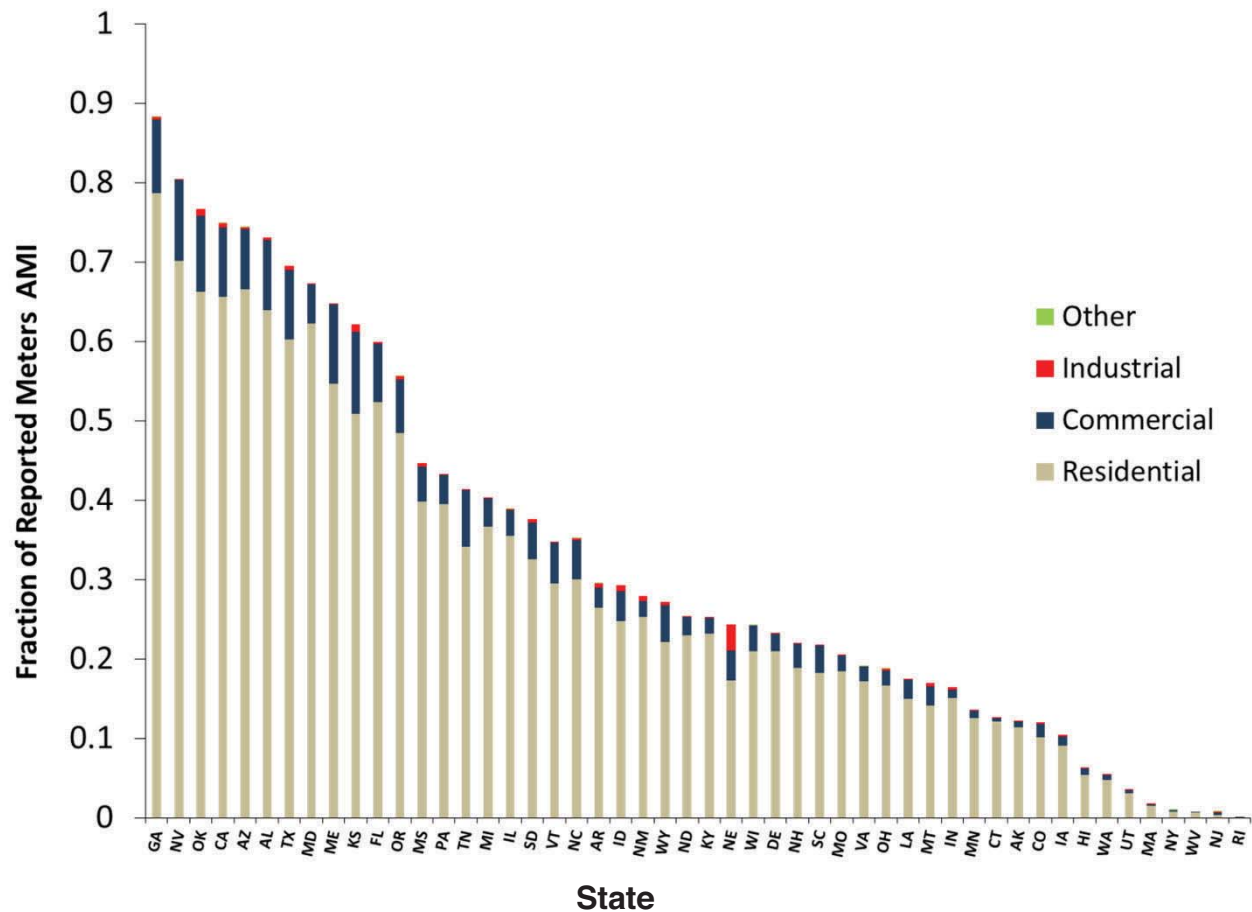
Compared to transmission systems, which have greater deployment of sensors and therefore provide operators with much better awareness of system behavior and operation, often local distribution utilities only monitor circuit breaker

status and measure feeder current and voltage as they leave the substation, and not at other locations on the circuit. However, some utilities installed automation sensing and fault current indicators on feeders themselves, although this level of monitoring is uncommon. Thus, most distribution utilities continue to rely on customer calls to assist in the location of faults. In the most rudimentary cases, utilities without distribution substation SCADA use customer calls to report outages and direct service restoration and repairs.

Utilities have yielded significant benefits from first-generation distribution automation, where cost-effective, but second-generation automation systems are still early in adoption (DOE, 2017b). One utility that adopted second-generation automation with the help of federal demonstration grants reported significant reductions in the severity and duration of outages, as well as economic and operational benefits (Glass, 2016). Of course, actions that increase automation, reliance on software, and communications infrastructure also add complexity and can inadvertently increase a utility's exposure and vulnerability to cyber attack.

Within the past decade, utilities have completed more than 60 million advanced metering infrastructure (AMI, sometimes also called "smart meter") installations across the United States. These investments were greatly accelerated by incentives arising from funding available in the 2008 American Reinvestment and Recovery Act. Figure 2.8 shows the percentage of electric meters with AMI by state. In distribution systems where it has been installed, AMI can provide information to assist in identifying the extent and location of customer outages, as well as the primary benefit of reducing the cost of meter reading. However, the outage data from AMI systems tend to be of poor quality and inconsistent for use in real-time fault identification and initial restoration. This is in part because the messages sent to operators are a "last gasp" from a meter losing power, and often the message itself cannot get back to the operations center as the communications network also loses power (most AMI systems installed are based on radio frequency mesh communications networks). As a result, most AMI systems today are used to validate that electricity service to customers has been restored and for postmortem analyses. More advanced AMI systems, which are available today, have addressed this issue and will be able to support real-time operational restoration and improved communication with customers. Furthermore, to take full advantage of AMI, utilities must make substantial investments in database management and analysis software to utilize the large amount of data flowing back to operators.

Deployment of advanced meters has been met with mixed reactions. Some state regulators remain skeptical of the benefits of AMI or contend that equivalent benefits can be achieved at a lower cost to customers (Reuters, 2010; AEE, 2015; NJBPU, 2017). Some customers have been suspicious of technologies that they view not only as expensive, but also



**FIGURE 2.8** Fraction of customer meters with advanced meters by state in 2015.  
SOURCE: EIA (2016a).

as potentially dangerous for their health<sup>15</sup> and for the security of their private data (Karlin, 2012; Spence et al., 2015). AMI roll-outs in some communities have experienced backlash for these reasons, although other AMI deployments have been much smoother.

Inverters convert the DC signal produced by solar panels or batteries to the AC power used on the distribution system and serve as the interface between many DERs and the distribution system. While the main task of an inverter is as an electric power conversion device, modern technology permits inverters to perform a broader array of ancillary tasks, which can be leveraged in power conditioning to support the grid in various ways (these are sometimes referred to as “Smart Inverters”). Currently, inverters operate with a spectrum of capabilities—for example, some are able to stay connected and ride through disturbances (and in some cases can contribute to solutions), while others automatically disconnect during a disturbance. Interim standards issued by

the Institute of Electrical and Electronics Engineers (IEEE) allow for such “ride through” of disturbances, and FERC now requires this capability. These standards remain under revision (IEEE, 2013).

Currently, relatively few of the inverters installed on the system can provide the local utility with visibility into the power injection of the DER into the grid or the ability to control it when necessary. At some point in the near future, when technical standards catch up with technology, it is possible that inverters will have the capability to communicate with utilities and system operators. This can be further leveraged to enhance system resilience under abnormal situations—for example, by changing inverter settings on the fly for adapting to changing grid conditions. Additional details are provided in the discussions in Chapters 4 and 5.

**Finding:** There is wide variation across the United States in the level of technological sophistication, penetration of sensors, deployment of advanced communications technologies, and level of automation deployed by distribution utilities. Many utilities, particularly in metro areas with overhead infrastructure, have invested significantly in first-generation automation over the past 30 years. Where cost-effective,

<sup>15</sup> While the field strengths are miniscule, the concern is with the possibility of health consequences from exposure to the RF communication associated with the AMI. Similar concerns are expressed by some people about a wide range of RF sources in the world today.

more advanced automation is beginning to be implemented to enhance reliability, resilience, and integration of DERs.

**Finding:** Actions that increase automation and reliance on software and communications infrastructure also add complexity and can inadvertently increase a utility's exposure and vulnerability to cyber attack. This is particularly acute with regard to DER integration.

Keogh and Cody (2013), researchers with the National Association of Regulatory Utility Commissioners (NARUC), explain the following:

[The regulatory] frameworks used to evaluate reliability investments are not perfectly equipped to address investments dealing with these large-scale and historically unprecedented hazards, and some improvements to the frameworks may be needed [p. 1]. . . . Those metrics miss two components: (1) They often undervalue the impact of large-scale events and focus on normal operating conditions; and (2) they price lost load at a flat rate, when in fact the value of lost load compounds the longer it is lost [p. 7]. . . . [M]aking every corner of our utility systems resistant to failure may prove cost-prohibitive, resilience should be selectively applied to the areas that need it most. Existing risk management frameworks can be better deployed to help prioritize where the best investments can be made. A resilience investment may be particularly valuable in the face of high-impact disasters and threats that utility systems have not faced before, like national-scale natural disasters or man-made cyber and physical attacks [p. 1].<sup>16</sup>

Thus, because the existing reliability metrics used to inform regulatory decision making are inadequate for informing resilience investments, continued research is needed to develop analogous metrics for electricity system resilience. Some regulators have begun to consider how resilience objectives should be incorporated by utilities in their jurisdictions, with several prominent examples promising to transform the electric industry today. In response to Superstorm Sandy, for example, New Jersey regulators approved more than \$1 billion in storm-hardening investments for critical substations and building additional distribution circuits for greater redundancy (NJBPU, 2015).

**Finding:** The decisions made by state public utility commissions and the boards of public or customer-owned utilities have significant influence on the reliability, cost, and resilience of distribution systems. The committee agrees with a NARUC analysis that concludes that techniques for guiding

and approving reliability investments are inadequate for resilience.

## METRICS FOR RELIABILITY AND RESILIENCE

### Reliability Metrics Are Relatively Mature and in Widespread Use

Reliability has long been a component of utility planning and operation, and there are many mature metrics to quantify reliability and evaluate potential reliability improvements associated with different grid investments. Reliability metrics are grouped into those applied to generation and transmission systems (e.g., adequacy, loss of load probability) and those for the distribution system, with common examples defined in Box 2.2. Metrics for generation and transmission are used by FERC and NERC, whereas oversight of reliability at the distribution level is left to state regulatory agencies. As previously discussed, ownership and operation of the U.S. electric system is characterized by a mixture of public, private, and cooperative institutions with different incentives and organizational structures, and these different institutions are regulated differently. Thus, different organizations are responsible for maintaining different packages of standards in different locations, some of which can only be attained through collaboration with others.

While reliability metrics are more established and widely used than resilience metrics, there remain many opportunities to improve their formulation and utilization. Although valuable, distribution system metrics that present average values lack details regarding the types of customers experiencing an outage and the severity of individual outage events. Thus, there is a need to increase the granularity of reliability metrics, and the Department of Energy (DOE)-sponsored Grid Modernization Laboratory Consortium (GMLC) is in the process of developing metrics for distribution reliability with greater spatial and temporal resolution (GMLC, 2017). Another critical opportunity for improvement is to better connect reliability metrics to the economic benefits of more reliable service, which requires an understanding of how different customers value reliable electric service.

As society becomes ever more dependent on continuous electricity supply, and the technologies and institutional structures employed to provide that service evolve, it is important to rethink the system's reliability criteria. To the extent that electricity supplies become more distributed, micro-sized local supply communities may take care of their own unique local needs; but to the extent that a significant component of supply is provided over a regional power grid, all users share equally in that bulk supplier's reliability (what is defined as a "public" good by economists) and so some centralized authority is needed to set and enforce the reliability standard for that supply entity. That standard could be based and routinely updated on some systematic estimate of the value of its reliability (and resilience, too).

<sup>16</sup> The authors also explain, "If an investment avoids or minimizes service interruptions in the absence of an extraordinary event, it is just an everyday reliability investment, and the means already exist for utilities and regulators to thoroughly consider it. An important point . . . is that resilient infrastructure does more than one thing well, because a resilience investment needs to pay for itself and create value for ratepayers, even when it is not being used" (Keogh and Cody, 2013, p. 5).

## BOX 2.2

### Common Distribution System Reliability Metrics

#### SAIFI

“System Average Interruption Frequency Index (Sustained Interruptions)—This is defined as the average number of times that a customer is interrupted during a specified time period. It is determined by dividing the total number of customers interrupted in a time period by the average number of customers served. The resulting unit is ‘interruptions per customer’” (APPA, 2014).

#### SAIDI

“System Average Interruption Duration Index—This is defined as the average interruption duration for customers served during a specified time period. It is determined by summing the customer minutes off for each interruption during a specified time period and dividing the sum by the average number of customers served during that period. The unit is minutes. This index enables the utility to report how many minutes customers would have been out of service if all customers were out at one time” (APPA, 2014).

#### CAIDI

“Customer Average Interruption Duration Index—This is defined as the average length of an interruption, weighted by the number of customers affected, for customers interrupted during a specific time period. It is calculated by summing the customer minutes off during each interruption in the time period and dividing this sum by the number of customers experiencing one or more sustained interruptions during the time period. The resulting unit is minutes. The index enables utilities to report the average duration of a customer outage for those customers affected” (APPA, 2014).

#### CAIFI

“Customer Average Interruption Frequency Index—The average frequency of sustained interruptions for those customers experiencing sustained interruptions” (APPA, 2014).

#### MAIFI

“Momentary Average Interruption Frequency Index—Total number of momentary customer interruptions (usually less than five minutes) divided by the total number of customers served” (APPA, 2014).

It is important to note that reliability metrics provide only limited insight about resilience. A survey of publicly owned utilities in 2013 indicated that two-thirds of the responding utilities excluded outages caused by major events when calculating their performance on reliability metrics (APPA, 2014).<sup>17</sup> Thus, planning, operational strategies, and technologies used to reduce impacts and expedite recovery from large-area, long-duration outages may have no impact on a utility’s performance measured by reliability criteria.

### Development of Metrics for Resilience Lags Behind Those for Reliability

Unlike reliability, there are no generally agreed upon resilience metrics that are used widely today. This is in part because there is not a long history of large-area, long-duration outages that can be analyzed to guide future investments (which is the case for reliability). Nonetheless, the electricity

sector is arguably more advanced in considering and evaluating resilience than other critical infrastructure sectors. There are myriad resilience metrics proposed in research and most remain immature (Willis and Loa, 2015). Some recent analyses have proposed resilience metrics based on concepts like resistance, brittleness, and dependency. Following the resilience processes introduced in Chapter 1, Kwasinski (2016) proposes that resilience is an attribute with four distinct metrics: (1) withstanding capability, (2) recovery speed, (3) preparation/planning capacity, and (4) adaptation capability. A study at Sandia National Laboratories lays out a broad framework for developing resilience metrics, frequently in combinations, and for valuing their respective contributions to overall customer value (SNL, 2014). Furthermore, individual utilities frequently establish their own metrics to guide decision making. For example, the committee was briefed by the Chicago utility Commonwealth Edison on metrics used in selecting optimal locations to site community microgrids,<sup>18</sup> based on a weighted sum of measures of

<sup>17</sup> Also, of the 180 utilities responding to the American Public Power Association survey, 87 percent collected outage data at the system level, 47 percent also collected data at the feeder or circuit level, and 31 percent collected data at the substation level (APPA, 2014).

<sup>18</sup> A microgrid is an energy system consisting of distributed generation, demand management, and other DERs that can connect and disconnect from the bulk power system based on operating conditions.



customer criticality, historical reliability, projected capacity constraints, and measures of substation health.

As part of the GMLC metrics analysis, researchers from multiple national labs proposed a set of resilience metrics, shown in Table 2.2, that build on a resilience analysis process developed as part of the DOE Quadrennial Energy Review. Because many causes of large-area, long-duration outages have a low probability and their impacts are highly uncertain (e.g., based on the types of customers impacted, the exact tract a hurricane follows), the GMLC metrics analysis emphasizes inclusion of statistical measures of uncertainty alongside reporting of resilience metrics and all consequences are estimated as probability distributions.

Development of resilience metrics and methods to defining resilience goals, as well as comparison of alternative strategies for increasing resilience, remains an active area of research, and the committee believes more research and demonstration is required before the electricity sector can reach consensus on a set of appropriate metrics. Metrics often drive decision making. Establishing and building

consensus around metrics is an important prerequisite for comparing resilience enhancement strategies and for evaluating their costs and benefits. Many of the technologies and strategies for increasing the resilience of the electricity system described in the following chapters are expensive, particularly when implemented on a large scale. Without consistent resilience metrics, large amounts of money could be spent with little understanding of actual resilience benefits and with much of this cost passed on to ratepayers.

### Economic Valuation of Resilience

Metrics for resilience should not be selected merely because they can be quantified easily. In deciding what level of resilience is appropriate, it is important at a minimum to estimate how much a lack of electricity system resilience costs individuals and society. Thus in developing resilience metrics, it is essential to be able to link those measures to the value retained or added to society. Furthermore, market responses and/or survey results may provide inadequate measures of resilience since they have attributes of both a private and a public good (many neighbors share the same benefit). Likewise the services provided by most public or private regulated utilities are combinations of pure public and private goods. This is why standards and regulations are important to maintain and restore quality in electricity markets, which are not classical competitive markets with fully rational decision makers (Hirschman, 1970).

Thirty years ago, with most electric supply utilities vertically integrated, the customers knew who to blame for outages. If the overseeing public utility commission (PUC) did not set and enforce adequate reliability standards, the resulting public outcry often resulted in a government response including public pillorying and/or financial penalties assessed against the responsible utility. In some instances of major outages, the outcry extended to elected officials in state or federal government. The principal example is the 2003 blackout that led to EPAct of 2005, granting new authority to FERC to set reliability standards for the bulk power system and to assess penalties for non-compliance.

Developing and enforcing resilience and reliability metrics will become increasingly complicated as technologies and customer preferences evolve alongside changes in public policies regarding equity and environmental goals. The emergence of competitive markets in some areas of the country has altered the institutional structure of the industry, the nature and form of its regulation, and the structure of its financing. So while competition has replaced regulation in some segments of the industry as the means of ensuring reasonable price levels, maintaining the reliability of the whole system has become more complicated with divided responsibility. At the bulk power supply level today, reliability standards are still maintained, but this is often done through market mechanisms that induce sufficient prices for

**TABLE 2.2** Example Resilience Metrics Proposed by the Department of Energy-supported Grid Modernization Laboratory Consortium

Consequence Category	Resilience Metric
<b>Direct</b>	
Electrical service	Cumulative customer-hours of outages
	Cumulative customer energy demand not served
	Average number (or percentage) of customers experience an outage during a specified time period
Critical electrical service	Cumulative critical customer-hours of outages
	Critical customer energy demand not served
	Average number (or percentage) of critical loads that experience an outage
Restoration	Time to recovery
	Cost of recovery
Monetary	Loss of utility revenue
	Cost of grid damages (e.g., repair or replace lines, transformers)
	Cost of recovery
	Avoided outage cost
<b>Indirect</b>	
Community function	Critical services without power (e.g., hospitals, fire stations, police stations)
	Critical services without power for more than N hours (e.g., N> hours or backup fuel requirement)

SOURCE: GMLC (2017).



adequate generation to be built at needed locations, as well as for generation operators to provide operating reserves and to be available to offer those services (provide adequacy), all as overseen by FERC. At the distribution level, state regulation (and public outcry) is primarily relied upon to sustain the reliability to end-use customers.

In the end, reliability and resilience are for the benefit of the customer and society, and all actions, including rules and regulations, need to reflect customer values. Although a consistent principle should be developed for the nation, cost-effective instruments are likely to vary widely. The application of the principle should take into account variations in climate, nature of hazards, socio-economic and demographic patterns, and the nature of customers (industrial, commercial, residential, essential public services, etc.), all of which may lead to different distribution-system configurations (e.g., there are mesh network designs in some densely populated areas, whereas less populated areas have radial distribution system designs).

No rule is effectively implemented without rewards or penalties assigned for adherence. For private goods, if there is truth in labeling and no hidden defects are possible, the market can take care of those incentives. In the case of public goods furnished by a unique provider in each location, assessing penalties for non-compliance can have pernicious repercussions if the service must be sustained. If compliance requires substantial capital investments, arranging financing can be challenging if the entity is under attack by its regulators and its next period's earnings promise to fall because of the fines. If fines are pooled over a wide area of providers in order to support resilience and reliability investments, there is little incentive for the individual utility to provide reliable service. The nature of such problems will change if numerous local microgrids and community-based distribution consortiums become widespread. Furthermore, the shifting of reliability and resilience decisions to the local level also presents serious challenges for financing. One model might be parallel to the U.S. Department of Agriculture Rural Utility Service's (RUS's) funding of rural cooperative electricity suppliers.<sup>19</sup> In the end, regardless of the form of the institution, reliability and resilience begins at home—at the distribution level with the customer.

Because electricity customers value *both* the reliability and resilience of the system, developing metrics and incentives (or disincentives) for utilities based upon resilience and reliability separately is likely to be sub-optimal. It is important that the possibility of trade-offs between resilience and reliability is integrated into metrics, and that the costs of supplying the sum of the measures do not exceed their combined value to customers and to society as a whole (SNL, 2014). At present, such an overarching valuation of

the burgeoning number of reliability and resilience metrics does not exist to aid in the development of reasonable and enforceable standards.

In addition to developing better resilience metrics and using them to monitor and realize better outcomes, knowing much more about what individuals and society are willing and able to pay to avoid the consequences of large-area, long-duration grid failures is an important input to deciding whether and how to upgrade systems to reduce impacts of an outage. Much of what we know is anecdotal from looking backwards at such failures, such as from Katrina, Sandy, or the Northeast blackout of 2003. Most prior quantitative studies have only examined outages of much shorter duration. Willingness and ability to pay may differ substantially based on geography, electric customer class, and socioeconomic status. So work should proceed in parallel to develop better metrics and a better understanding of consumers' and society's willingness to pay.

**Finding:** While reliability metrics are relatively well established and widely used in electricity system planning and operation, the development of agreed-upon metrics for resilience lags significantly behind. Further, since there is currently no common basis for assessing the relative cost-effectiveness of the existing reliability metrics that differ by purpose, integrating the ongoing work on developing resilience metrics may lead to confusion and duplication in their implementation. Thus it may be difficult to evaluate, compare, and justify investments made to improve resilience and to assess progress made in enhancing both the resilience and the overall reliability of the grid.

**Recommendation 2.1:** The Department of Energy should undertake studies designed to assess the value to customers—as a function of key circumstances (e.g., duration, climatic conditions, societal function) and for different customer classes—of assuring the continuation of full and partial (e.g., low amperage and/or periodic rotating) service during large-area, long-duration blackouts.

**Recommendation 2.2:** The Department of Energy should engage the North American Electric Reliability Corporation, the National Association of Regulatory Utility Commissioners, the National Rural Electric Cooperative Association, and the American Public Power Association in a coordinated assessment of the numerous resilience metrics being proposed for transmission and distribution systems and seek to operationalize these metrics within the utility setting. That assessment should focus on how system design, operation, management, organizational actions, and technological advances are affected by those metrics. All metrics should be established so that their cost-effectiveness in bringing added value to the nation can be assessed. Complementarities between metrics should be identified, and double counting of their effects should be avoided.

<sup>19</sup> The RUS provides loans and loan guarantees to help finance construction and operation of electric distribution and transmission systems (among other things) in rural areas. Electric cooperatives (and other utilities) may receive such financial support from the RUS (USDA, 2016).

## NEAR-TERM DRIVERS OF CHANGE AND ASSOCIATED CHALLENGES AND OPPORTUNITIES FOR RESILIENCE

As described previously, significant transitions are currently under way in the power system and its associated institutions. Some changes result from market fundamentals including changing customer preferences, others from an array of state and federal policies, and yet others from technological innovations that offer both opportunities and new challenges for the grid, especially in terms of resilience. The future electric system will have a more complex array of central-station power plants on the bulk power system, as well as DERs behind customers' meters or otherwise attached to the local distribution system. Many more players will use technologies and applications that can expose the grid to greater risk of cyber attack. These changes may both facilitate and complicate the development of greater reliability and resilience. Starting with a description of these various trends that are affecting the grid, this section discusses some of the implications of those trends for the resilience challenges its owners, operators, and users will increasingly face in the years ahead.

### Power Market Fundamentals

The nation's "shale gas revolution" began a decade ago and has contributed to a changing generation mix in many parts of the United States, particularly where coal-fired or nuclear generation have been major players. In combination with a decade of flat electricity demand (EIA, 2016b), loss of cost advantages for coal (Tierney, 2016a), declining costs for small-scale and utility-scale wind and solar generating technologies (Lazard, 2015), and controls on emissions of mercury and other toxic air pollutants, this has contributed to retirements of 49.3 gigawatts (GW) of coal-generating capacity since the year 2000 (EIA, 2016c). Most of these plants were older, relatively inefficient, and without modern pollution controls. Because of competition from low-cost natural gas and the high costs of plant life extensions, several nuclear plants have been retired in recent years with others facing premature closure (BNEF, 2016).

The vast majority (91 percent) of the 403 GW of generating capacity added since 2000 has been at gas-fired generating units (281 GW), as well as wind and solar installations (together, 87 GW) (EIA, 2016d). In 2016 alone, utility-scale wind, solar, and gas-fired capacity amounted to 93 percent of total generating capacity additions (EIA, 2016d). Another 2 GW of distributed solar capacity was added in 2015, which is the most recent year reported by EIA (EIA, 2016e). The changing electric generating mix is introducing new challenges for grid operators, who must keep generation and consumption balanced with a decreasing amount of baseload coal and nuclear assets and an increasing share of intermittent, non-dispatchable generating resources.

DERs differ from the large central generators that traditionally form the backbone of the grid in that DERs are much smaller, located closer to consumers, and often controlled in a decentralized fashion by local users themselves. The shift to DERs comes as a result of changes in technology, customer preference, and policy. Technologically, numerous new power supply, response, and control systems are emerging. At the same time, federal and state regulators, as well as others, are pushing for the adoption of DERs with a variety of goals that are described further in Box 2.3 and in the following section. As with almost any change in technology, these driving forces interact in many complex ways. Some of the changes in technology are purely exogenous, but most are responding at least partly to policy signals. These forces also interact with consumer preferences, as is typically observed with changes in other technologies. New technologies for local supply and power conditioning have seen early adoption by users who have a particularly strong preference for reliable power, such as hospitals and server farms.

### Federal and State Policy Drivers

The federal government and most states have been active in adopting policies aimed at promoting the introduction of efficient and renewable energy technologies, controlling emissions associated with power generation, and fostering innovation and grid modernization. These policies, many of which are mentioned in Box 2.3, have impacted both the bulk power and local distribution systems. Importantly, but with notable exceptions, federal and state policies that have encouraged development of advanced technologies and DERs have been motivated by considerations of economic development, environmental impacts, or clean-energy goals, rather than by concerns for resilience and reliability.

While many of these federal and state policies have been directed toward regulated utilities, many have encouraged non-utility entrants to make investments, operate programs, and bring new technologies to the marketplace. Today, many of the devices (e.g., central-station power plants, rooftop solar installations and their accompanying smart inverters) attached to the grid are owned by third parties. There are many more actors affecting the operations of the grid, and grid operators and others need to take into account a wide variety of facilities and resources as they assure the operational reliability and security of the grid.

To gain a better appreciation of the state of DER and microgrid adoption in jurisdictions across the country, the committee sent a questionnaire to public utility commissions in all 50 states and the District of Columbia and received nearly 25 responses. The questionnaire sought anecdotal information about variations in deployment of smart meters, distribution automation, organized DR programs, CHP facilities, and questions regarding legal constraints on microgrids across the country. Answers called attention to wide differences in adoption of these technologies and views on their

### BOX 2.3

#### Federal and State Policy Drivers of Change in the Electric System

##### Federal Drivers

- Encouraged the development of alternative energy produced by non-utility generation (e.g., PURPA in 1978);
- Promoted competition in wholesale electricity markets (e.g., through the EPActs of 1992 and 2005);
- Mandated the introduction of increasingly efficient electric appliances into the marketplace;
- Supported utilities' investments in advanced meters and other technologies (e.g., through the American Recovery and Reinvestment Act of 2009);
- Required mandatory reliability standards and authorized incentive rate of returns on some transmission investments on the bulk power system (both under the EPAct of 2008);
- Introduced investment and production tax credits for renewable electricity;
- Adopted new regulations under the decades-old Clean Air Act to control air toxic and carbon-dioxide emissions from existing fossil-fuel generators; and
- Standardized small generator interconnection procedures.

##### State and Local Drivers

- Opened retail commodity markets to competition and third-party innovation (see Figure 2.6);
- Encouraged the development and adoption of renewable resources (DSIRE, 2016a, 2016b, 2016c);
- Developed state tax incentives for energy efficiency and renewable energy (DOE, 2016b; DSIRE, 2016d);
- Installed advanced metering devices and microgrids in New York and California, for example (Tierney, 2016b);
- Developed rate designs (such as net metering<sup>a</sup> tariffs or time-of-use rates) to encourage DER adoption;
- Implemented energy efficient appliances, green buildings, and other measures to increase the efficiency of energy use (ACEEE, 2012; Alliance to Save Energy, 2013);
- Promoted adoption of electric vehicles and installation of the charging infrastructure to support them (Plug-in America, 2016); and
- Adopted technologies to control carbon emissions from power plants (RGGI, 2016; CARB, 2014).

<sup>a</sup> Net metering is a billing arrangement in which a customer with distributed generation receives credit for the energy he/she provides to the grid, sometimes at full retail rates or a fraction thereof.

potential to increase system reliability and resilience across the United States, as summarized in Box 2.4. Although not quantitative and not used to make any comparative statements, the answers received by the committee broadly align with previous studies done by FERC (2016b) and stakeholder groups (Gridwise Alliance, 2016).

#### Changing Time Scales for Grid Operators

Along with the changes to the fundamentals of the generation mix, the electricity power system is undergoing changes to the time scales for operations, especially in the area of power markets for restructured utilities. The future will see continued shortening of time scales for grid operations: data on system conditions come in on time scales under a second, and the dispatch of resources and market settlements happens every 5 minutes. The requirements for such rapid dispatch and analysis have impacted the tools used to manage the system, causing the energy management systems within RTOs to be custom built. The operational concerns of the collapsing time frames and the human interface are real. Though

the resilience impacts of these changes are complex, these challenges motivated the committee to recommend research on improvements to system operator control rooms and the application of artificial intelligence to power system monitoring and control within Chapter 4. These concerns also help motivate overarching recommendations to improve the security and resilience of the cyber monitoring and controls systems within Chapter 7.

#### Industry-Structure and Business-Model Transitions

There are new industry structure and business model issues that are also in transition, with uncertainty about which direction they will take in the future (NASEM, 2016; MIT, 2016). Competitive forces, often stimulated by actions of federal and state legislatures and regulators, have prompted an array of new actors (e.g., non-utility generating companies and independent non-utility transmission companies), new institutions (e.g., RTOs and ISOs), and new issues subject to FERC regulation in wholesale electricity markets and the bulk power system. Most of these institutional changes have

### BOX 2.4

#### Example Comments to the Committee on Distributed Energy Resource and Microgrid Deployments Across the United States

Staff of the Pennsylvania PUC noted that “there are no utility-owned or operated microgrids in Pennsylvania at this time. However, there are some campus and commercial test beds, especially in the Philadelphia and Pittsburgh areas. . . . The Pennsylvania PUC encourages distribution utilities to make use of advancing technologies and support CHP projects. Smart meters are mandated for all large electric distribution companies.”

The New Jersey Board of Public Utilities was the only state utility regulatory organization that indicated a microgrid was able to sell electricity directly to “one customer across one right-of-way,” as well as being able to sell power into the wholesale market operated by the RTO PJM.

The Georgia Public Service Commission (PSC) described major investments made by Southern Company in advanced metering and distribution automation: “The resulting smart grid network will greatly improve reliability for Southern Company customers. . . . Georgia Power reports its reliability statistics (SAIDI, SAIFI) annually since 2003. Since the installation of the smart grid equipment, these metrics have trended downward.”

According to staff of the Illinois Commerce Commission (ICC), “The Illinois General Assembly has enacted laws, and the ICC has adopted ratemaking policies that support and encourage the development and deployment of new technologies and facilities. Utilities report that their actions combined with customers’ responses to programs tied to new technologies result in reliability and resiliency improvements.”

In Kansas, the state Corporation Commission staff responded, “So long as these technologies are dispatchable by the incumbent utility, staff views them as supportive of system reliability and resiliency.”

Staff of the North Carolina Utility Commission informed the committee, “The Commission encourages utility consideration and deployment of cost-effective new technologies that would improve the reliability and resiliency of the electric grid. The utilities are required to address these technologies in their integrated resource plans and smart grid technology plans filed with, and reviewed by, the commission.”

The Montana PSC staff indicated, “The PSC supports regulated utilities to engage in pilot projects and studies to gain insight into potential benefits of [advanced DER] technologies.” One utility in their jurisdiction is “currently engaged in a smart meter pilot project with some use of distribution automation.”

Staff of the Idaho PUC told the committee that advanced DERs and automation technologies “improve outage control, system monitoring, and reduction in system peaks to reduce overall costs.”

Staff from the Iowa Utilities Board indicated, “With market refinements, these technologies enable the utilities to flatten the demand (load) curve by passing appropriate price signals. Proper price signals result in build-up of generation only as needed and thus improve system reliability and resiliency.”

Staff of the Delaware PSC noted that there are “a few installations where [distribution] feeders are automatically reconfigured upon loss of service. These installations are limited to critical service customers such as sewage pumping or water pumping stations.” Staff went on to say that “reliability and resiliency need to be balanced with the costs that ratepayers will incur with the new technologies.”

In Wisconsin, PSC staff explained that they have “not taken any formal action related to the ability of these technologies to improve grid reliability and resiliency. . . . Wisconsin utilities typically have good reliability indices and high customer satisfaction, and [advanced DER technologies] do not necessarily result in improvements in SAIFI, SAIDI, and CAIDI, so it is difficult to measure how these technologies directly affect reliability.”

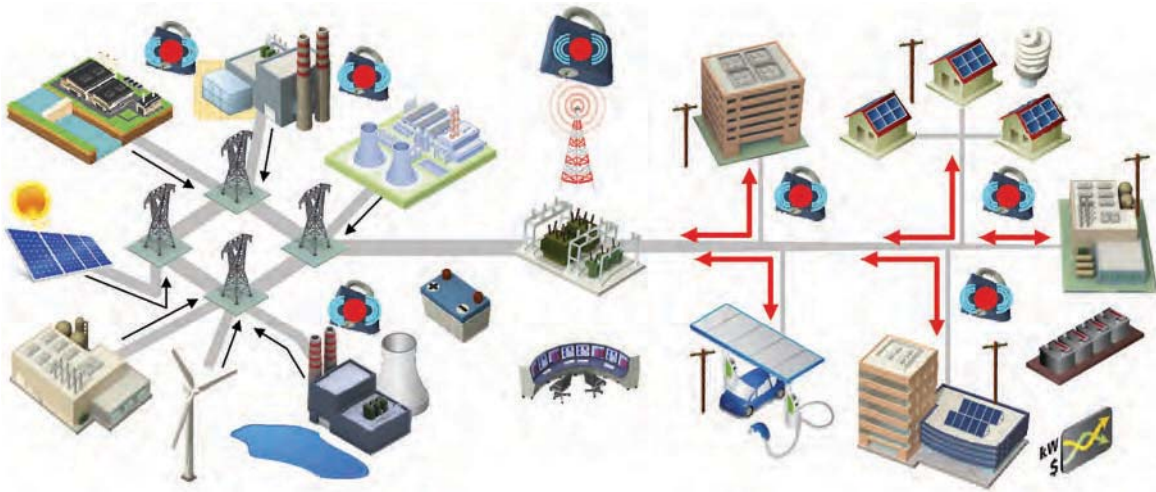
The Regulatory Commission of Alaska observed, “The electricity infrastructure in Alaska differs from that in the lower 48 states in that Alaskans are not linked to large, interconnected grids. . . . Most of the state’s rural communities have no grid access and rely on community electric utilities to provide service via diesel generators.”

already occurred. Unlike the bulk power system that has undergone significant restructuring and regulatory reform over the past decade, the structure and regulation of electric distribution systems has, until recently, experienced much less change. Thus, the committee considers that the largest changes to the structure of the electricity system in the future will occur within the distribution side of the system.

At the distribution-system and retail electric level, the relatively rapid emergence of DERs has accelerated pressure on regulators, utilities, and other stakeholders to address aspects of the traditional utility business model, which has supported grid investments largely through rates that recover significant

quantities of utilities’ fixed costs through usage-based charges. All else equal, as new small-scale technologies generate power from customers’ premises and inject it into the grid (Figure 2.9), causing revenues from volumetric rates charged to customers to drop, utilities and others have begun to look for regulatory frameworks and new rate designs that assure that all customers pay their fair share of the costs of maintaining a reliable and resilient grid. The approaches under discussion across the country for the future roles of the local distribution utility include the “enhanced status quo,” the “network service provider,” the “market enabler,” and the “solutions integrator” (De Martini and Kristov, 2015; State





**FIGURE 2.9** Schematic of possible electric system configurations and interactions in the future.  
SOURCE: EPRI (2011).

of New York, 2014; Tierney, 2016b; TCR, 2016). These new business models are relevant for resilience considerations in light of the fact that each poses different implications for the entity(ies) responsible for supporting resilience on the grid:

- *Enhanced Status Quo*. In this model, utilities will continue to manage their generation and/or delivery infrastructure to supply power to customers as today. At the same time, utilities will continue to invest in replacing aging infrastructure and advanced grid technologies to improve system reliability and resilience under traditional regulatory cost-of-service, ratemaking, and cost-recovery models (including revenue decoupling, in which utility cost recovery is delinked from volumetric electricity sales).
- *Network Service Provider*. As a more distributed energy future unfolds, the distribution system becomes a platform for enabling DERs to provide services to the wholesale market and as “non-wires alternatives” (so called because targeted installation of DERs can defer the need for transmission expansion). This model expands the role and value of the distribution system. This is accomplished by providing open access distribution services enabled by advanced technologies to allow the integration of high levels of DERs. Distribution services are based on network access fees comprised of demand charge and fixed charge components. Financial incentives for operational performance (e.g., for reliability and interconnections) and earnings mechanisms on DER non-wires grid services are employed. Otherwise, the traditional regulatory and utility economic model remains.
- *Market Enabler*. This model focuses on expanding the role of the utility distribution operations to become the distribution system (or market) operator (DSO).

This “total DSO” (De Martini and Kristov, 2015) has responsibility for balancing demand and supply as well as distribution network reliability for a distribution area to an interchange point with the bulk power system operator. In this role, the DSO provides a single aggregated interface with the ISO/RTO, requiring the DSO to optimally dispatch DERs within its area. Traditional regulatory and utility economic models apply, along with the incentives above and market-based pricing for optional competitive services.

- *Solutions Integrator*. This model focuses on developing customer DER assets alongside other energy services, such as power and natural gas commodity supply, energy information services, and energy efficiency retrofits. In this model, utilities provide turn-key or selected engineering, procurement and construction services to support reliability, enhancement projects, customer high-voltage infrastructure, microgrid, and DER implementation. Services may also include customized engineering and operational consulting as well as emissions management and equipment condition assessment to ensure safety and reliability.

A critical factor in the transitions of the electricity sector is that continuing reductions in the cost and accelerating deployment of DERs is leading to a new class of customer that is both an electricity consumer and producer (“Prosumer”). There are now large and small prosumers who are increasingly interested in managing various aspects of their own electricity usage and supply. This is also enabling greater customer choice for installing select DER technologies to satisfy individual customer requirements associated with reliability, redundancy, and power quality. Whereas most backup power requirements in the past relied on diesel generators, numerous other DER technologies can supplant



or even replace the diesel generator as a backup power option. However, DERs have complex impacts on resilience, which are discussed in the following sections and throughout the report.

### **Distributed Energy Resources and the Distribution and Transmission Systems**

DERs can provide benefits not only to the customers that employ them directly, but also to the broader transmission and distribution system. For example, DERs may help avoid or defer the need for new generation, transmission, or distribution infrastructure to address congestion, localized reliability, or resilience issues. The value of DERs for reliability, efficiency, and resilience depends upon their location and their particular attributes (e.g., their durability, their ability to be controlled, their availability when needed, the times of day when they reduce net load to the grid). Absent effective planning, DERs can also impose costs on the electricity system—for example, through equipment upgrades necessary to handle generation on distribution circuits, sub-optimal DER placement that contributes to congestion as opposed to alleviating it, and incomplete or inefficient sharing of information across the distribution-transmission interface.

This is particularly true at the distribution-system level, but also for interactions with the transmission grid. On the planning side, DERs can interact with the transmission system in several ways. First, behind-the-meter DERs complicate regional load forecasting, the process used to predict customer electricity demand at least 10 years into the future. Transmission system planners design the high-voltage system to meet forecasted demand. DERs behind the meter that provide energy to their owners have the potential to decrease load forecasts by the local retail utilities, which may account for DERs in their forecasting. Bulk power system planners may not be aware of DERs, and their load forecasts may not reflect the locations and types of DERs appearing or expected to appear on the system (NERC, 2016b).<sup>20</sup>

DERs can also be used in transmission-system planning processes to address specific system needs identified through modeling that informs planning. If a planned generating unit retirement or predicted demand increase may lead to a localized reliability issue, DERs could be employed to address that issue in lieu of a more traditional solution like a substation upgrade or new transmission line. Several legal, operational, and institutional barriers to employing DERs as transmission-system solutions exist, but the potential is real.<sup>21</sup> The use of DERs to address transmission-system

limitations may also increase resilience in that the resources are more readily available after an outage or disturbance that could knock out a substation or transmission line for significant periods of time.

On the market design and operations side, DERs also have implications for the transmission system. In addition to potentially reducing the capacity-procurement needs of a region, DERs are legally able to participate in wholesale energy, capacity, and ancillary service markets. These centralized markets exist only within the RTO and ISO regions shown in Figure 2.5; the rest of the transmission-owning utilities rely on bilateral contracting or self-supply to meet their electricity needs.<sup>22</sup> Some DERs have made progress in wholesale market participation. In PJM, for example, demand response resources participating in the wholesale market totaled more than 9,800 MW, with resources positioned at more than 17,000 locations across the PJM footprint (McAnany, 2017).

On both the transmission planning and wholesale market sides, a lack of operational awareness and coordination between distribution utilities (or, in the future, “distribution system operators”) and transmission-owning utilities, or the RTOs or ISOs operating the transmission system and wholesale power dispatch, serve as additional barriers to capturing the full potential value of DERs to the electric system. DER owners must understand what planning and market opportunities exist at both the distribution and transmission levels, and utilities and market operators must understand when resources are available for their use and when they are otherwise committed to provide grid services that render them unavailable for other uses.

**Finding:** The value of DERs for reliability, efficiency, and resilience depends upon their location, their attributes, the planning process behind their installation, and the legal and regulatory environment in which they are operated. While they can contribute to reliability and resilience, absent effective planning and an appropriate regulatory environment, DERs can also impose vulnerabilities and costs on the distribution system.

### **Other Technology Developments**

Other new and emerging technologies may have important impacts on the structure and operation of the power system, including lower cost batteries as well as falling cost and growing capabilities of power electronics. Energy storage in the distribution system and on the customer side of the meter is a relatively new phenomenon. Some distributed energy storage (DES) is provided by thermal systems such as

<sup>20</sup> For example, the RTO that covers 13 Mid-Atlantic states and the District of Columbia, called PJM, was able to decrease its load forecast by 6,000 MW for 2020 by incorporating the energy efficiency and distributed solar that exists or is planned to come online between now and then (PJM, 2016).

<sup>21</sup> See Southern California Edison and Consolidated Edison projects discussed in Tierney (2016b).

<sup>22</sup> One notable exception is the recent development of an Energy Imbalance Market (EIM) administered by the CAISO, with participation by a growing number of utility systems in the Western grid. As of 2017, several electric utilities in Arizona, California, Idaho, Nevada, Oregon, Utah, and Wyoming had joined or are planning to join the EIM (CAISO, 2017).

hot water heaters. Other DES technologies involve chemical (e.g., battery) solutions. There is large variation in projected battery costs, potentially declining from today's levels of about \$600/kWh for whole battery systems to the range of \$200–\$300/kWh by the early 2020s. Lower cost batteries are providing interesting opportunities. Customers are installing on-site battery systems behind the meter in service areas with high charges for peak power consumption to shift their usage to off-peak periods. In general, energy storage has the potential to enable the electric system to become more efficient while enabling customer-side energy management (Navigant Research, 2013).

Over the next 20 years, customers will likely have greater technological opportunities to go entirely off grid, satisfying their electricity requirements with a combination of on-site generation and storage technologies. Customers capable of investing in such packages of technologies (or purchasing such services from the utility or a third party) may be able to take personal responsibility for their own resilient electric service. Although the committee believes the share of total customers taking advantage of such approaches will be limited, trends in grid defection and the technologies that could enable it should be closely monitored. Broader impacts on social equity will also warrant attention.

The controllability of DERs is enabled by low-cost computing and communications technologies. The internet of things and edge computing have progressed to the point where the capability to control DERs at low cost has become much more practicable, with significant advances even over the past few years. There is also significant experience among a number of utilities and third-party aggregators implementing and operating “smart grid” technologies that include operation of distributed generation, storage, and demand response. Fundamentally, the computing and communications technologies are not the limiting factor for adopting these control strategies, although they will require increasing sophistication and resolution in the monitoring and control systems used at the individual feeder and substation scale to understand and optimize circuit health and behavior.

Most organizations that have employed various DER strategies on a large scale have discovered that the need for “big data” analytics and other strategies to optimize the operation and control of these distributed assets is nascent, and more effort is needed to further develop the algorithms to enhance system operations and resilience by managing DER deployment. This is particularly true during off-normal conditions where the DER might be providing emergency backup power to support system restoration. Finally, these DER assets will necessarily need to interact with each other seamlessly, including during normal and off-normal or emergency situations, and not create or exacerbate any adverse conditions. These include but are not limited to hazards to utility workers and the public, equipment damage, and sub-optimal operation of the remaining electrical assets.

## Interdependencies Between the Electric and Natural Gas Infrastructure

One outcome of the trends under way in the electric system is the industry's overall reliance on natural gas to fuel power generation, which increases the electric system's reliability on conditions in the gas industry. This has potential implications for the resilience of the grid. The conventional wisdom is that the electric industry will become even more dependent upon natural gas than it has in recent years, and the natural gas industry looks to a future in which significant growth in demand depends upon developments in the power sector. For the electric system to become more reliable and resilient, attention must be paid to assure robust systems and practices across the two industries.

For many years, these two systems developed on largely different paths, from physical, economic, engineering, institutional, industrial-organizational, and regulatory perspectives. Both industries evolved with some degree of vertical integration and with aspects of each industry's value chain regulated as monopolies by federal and/or state governments. The interconnected networks of each industry expanded over larger and larger geographic footprints. Recently, both systems have undergone eras of significant industry restructuring, with new players emerging as functions became unbundled and as competition entered into different parts of the business.

Today, however, each industry has its own set of cost structures, operating protocols and standards, commercial instruments, and pricing arrangements. Further, while the electric system operates as a network, following laws of physics on an interconnected grid rather than ownership or contract paths, the natural gas system is not a network industry. Individual companies own segments of the pipeline system, and users contract for access to and use of specific facilities. These changes also have occurred in parallel with dynamic developments in real-time, internet-based communications systems, complicating the interdependencies and allowing opportunities for new arrangements and solutions.

Today, natural gas supply still tends to move long distances from production sources to users' sites, typically to locations where there is little to no storage close to or on the end-user's property. This means that from an operational point of view, gas resources need to move “just in time” (i.e., they are used as they are delivered) to the end user through pipelines. During certain seasons and times of the day, many of these pathways—for example, those serving the Mid-Atlantic and Northeast regions—can become quite congested with firm gas deliveries, recognizing that gas injections at the production locations are intended to balance withdrawals of gas from the delivery system while taking in to account a variety of operational issues along the pathway from production to use. (“Just in time” delivery, however, sits within a context in which natural gas moves between 15–20 miles per hour on the interstate pipeline system, while

electric system operations occur at the sub-minute and multi-minute time frame.) Further, the growth in the power sector's use of natural gas has not been accompanied in all relevant regions by expansions in pipeline capacity or increases in the efficiency of existing gas delivery infrastructure. Without change in some of the key features in current business models for competitive generators or in market rules, that situation is not expected to change dramatically in the near term, making it difficult to drive investment in pipeline/storage infrastructure based on demand from the electricity sector. (In some regions such as New England, however, changes in market rules have led many gas-fired generators to invest in dual-fuel [oil/natural gas] capability with on-site storage of oil as a lower-cost means to assure the ability to operate during periods when delivery of natural gas over pipelines is otherwise constrained.)

Regulatory issues at the intersection of gas and electric markets are complicated. While FERC may have responsibility for a broad set of policy issues on electric/gas integration issues, and NERC is evaluating the interdependencies from an operational and planning perspective, the states have strong interests and, in some cases, regulatory responsibilities that can affect market participants' behaviors as well. Importantly, the structure of the natural gas production and delivery system in the United States does not have the same reliability requirements as now exist in the electric industry, and parts of that supply chain (e.g., production of natural gas) are effectively outside of FERC's regulatory jurisdiction.

The electric and gas systems are already experiencing strains at their intersection. To date, integration issues related to increased gas-fired generation have caused rotating power outages in the Electric Reliability Council of Texas during the big freeze of 2011. And, owing to winter gas shortages and extreme cold weather, natural gas was either unavailable or priced too high for generators in PJM and the New York ISO during the polar vortex of 2014 (see Box 4.2 for a description of these events). In some regions, for example, generators need to commit to move gas volumes before knowing whether their offers into the RTO's daily power markets have been accepted; conversely, generators need to offer prices into such energy markets without fully knowing the price and/or availability of their natural gas. There are other instances where gas customers that have contracted for firm gas supply and transportation service face potential (or real) curtailments as operational conditions change upstream and downstream. Tensions are visible across the business models of different players in the two industries and in the market rules in different regions. Further, there are different attitudes across the two industries regarding the urgency of anticipated changes in natural gas supply associated with growing use for electricity generation—specifically, the need for increased total supply and for that supply to be more nimble. It is difficult enough to introduce change into a single industry, where there may be players who perceive themselves as winning or losing from different options for

resolving small and large issues. It will undoubtedly be even more difficult to introduce sensible but meaningful changes affecting market participants in two industries.

Decisions by myriad market actors and institutions do not typically reflect coordinated information about the performance of systems either across industry segments (e.g., across the electric and gas industries) or within industry supply chains (e.g., from production sources across interstate transmission systems). In the context of the events that occur in one or more parts of the industries' systems, this absence of coordination mechanism may make some aspects of resilience—preparing for outages so as to limit their impact, sustaining service during an outage, and/or in restoring the systems to normal operations after the event—difficult to realize.

**Finding:** The electric industry has become highly dependent upon natural gas, and the natural gas industry looks to a future in which significant growth in demand depends upon developments in the electricity sector. For the electric system to become more reliable and resilient, attention must be paid to assuring the availability of adequate natural gas resources at all periods of time, including through investment in natural gas infrastructure (e.g., contractual arrangements and siting and construction of pipelines or storage), where it is economical to do so, fuel diversity for electric generators and natural gas compressors, and the alignment of planning and operating practices across the two industries.

### Emerging Electric Grid Jurisdictional Challenges

Historically, and despite the state-to-state and regional variations in grid regulation around the country, FERC, the states, and regulated utilities have operated within relatively clear jurisdictional boundaries. In an electric grid consisting predominantly of large and dispatchable central station power plants, it was clear that FERC had jurisdiction over wholesale electricity rates and interstate transmission, whereas states had regulatory authority over retail sales and delivery over local transmission and distribution systems into our homes, businesses, and industrial facilities. Power on the system generally flowed in one direction, from the generator all the way to the end-use customers.

Over the past decade, however, the increasing penetrations of DERs and smart grid technology that are relevant for resilience have begun to change the very way the grid operates (see Figures 2.1 and 2.9). The grid is increasingly an interconnected web rather than a straightforward series of one-way pathways. However, the federal, state, and other legal constructs dictating the role of DERs on distribution and transmission systems are in active review by FERC and states in the relevant regions. Although this is a constructive response, there remain many jurisdictional ambiguities, policy mismatches, and an inability to maximize the potential value of technological change toward grid reliability and

resilience. The emerging relationships between DERs and the transmission and distribution systems have greatly outpaced the laws and regulations that govern their interactions. The 80-year-old FPA never contemplated the modern and complex system that exists today. As a result, the relatively clear boundary between state and federal authority over the electric system has blurred to some extent, causing uncertainty, if not confusion, among policy makers and energy industry participants. Recent legal challenges taken up to the Supreme Court have begun to sort through aspects of unresolved jurisdictional questions, but several questions remain.<sup>23</sup>

Jurisdictional issues are also emerging within the distribution and transmission systems themselves. On the distribution system side, regulations typically assume one-directional power flow and fail to contemplate most DERs, including microgrids. From a resilience perspective, microgrids are a particularly interesting development—but they are not without legal uncertainties. Most state regulations obligate utilities to provide distribution service to all customers within their territories. With that obligation often comes the right to be the exclusive distribution provider. Microgrids that would connect buildings or a broader area technically involve their own distribution service and so, in many cases, are prohibited by existing utility regulations.

On the transmission system, the FPA itself remains a barrier to increased DER participation. For example, in the regional system planning processes, the FPA allows for transmission owners to allocate and recover the costs of new transmission investment except for non-wires alternatives, which includes DERs that are traditionally regulated by the states. As noted, the relationship among emerging technologies, evolving business models, and outdated laws and regulations that dictate authority over electric grid activities are stressed by the rapidly changing composition of resources and services involved with the delivery of energy, resulting

in significant uncertainty. This, in turn, creates challenges for resilience planning.

**Finding:** Any new local, state, or federal programs, regulations, or laws designed to increase grid resilience will have to navigate a labyrinth of existing state and federal laws (some of which are out of date) that shape the incentives (or disincentives) for undertaking investments and actions aimed at enhancing resilience. This creates challenges for resilience planning, especially in light of the essential role of electricity in providing critical services and powering the economy.

## LONGER-TERM DRIVERS OF CHANGE AND ASSOCIATED CHALLENGES AND OPPORTUNITIES FOR RESILIENCE

There is, of course, no way to reliably predict what the power system will look like in 30 to 50 years. However, it is possible to identify a variety of developments that could shape that future and then seek strategies that will be robust across that range of possibilities. To that end, here the committee identifies and discusses a variety of factors that might shape the future evolution of the system. Planning for grid resilience needs to take into account the expectation that the grid and its various institutions, technological features, legal structure, and economics will change—and in ways unknown today.

### The Nature and Scope of the Future Regulatory Environment

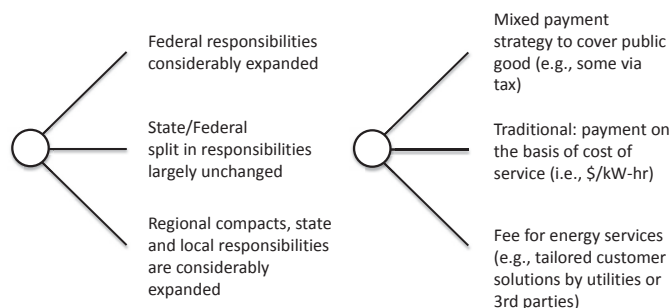
Recent years have witnessed a dramatic shift in the structure and regulatory environment in which the high-voltage transmission system operates. A similar transformation has not yet occurred at the level of the distribution system. Whether such a transformation will occur, and what form it might take, will likely have profound effects on the future evolution of the system. Will federal authority be expanded to include a larger role at the level of the distribution system (Figure 2.10), as could occur, for example, where customers with on-site generation sell surplus back into the grid and thus set up the possibility of federal jurisdiction where such injections of power were considered sales for resale? Many states would likely oppose such an expansion, in a continuing tension between state and federal oversight seen in previous legislation including various provisions of PURPA and EPCRA 2005.<sup>24</sup> The latter specifies the following:

Each electric utility shall make available, upon request, interconnection service to any electric consumer that the electric utility serves. For purposes of this paragraph, the term “interconnection service” means service to an electric consumer under which an on-site generating facility on the consumer’s premises shall be connected to the local distribution facilities. Interconnection services shall be offered based

<sup>23</sup> These recent cases have clarified a few different jurisdictional principles: First, one Supreme Court decision called *EPSCA v. FERC* determined that FERC has the authority to regulate DER participation in wholesale markets. This authority means that, under certain circumstances, states and the federal government will both have the ability to regulate DERs in the performance of different activities. Second, another high court decision (known as *Hughes v. Talen Energy Marketing, LLC*) recognized that states have the authority to engage in their own preferred resource procurement efforts, but that they cannot cross a line that would invade FERC’s exclusive authority to set wholesale energy rates. The *Hughes* decision has fewer direct implications for DERs that may be procured for resilience purposes than it does for supply-side generating resources like wind, solar, or natural gas power plants, but it is nonetheless important to keep in mind in resilience program design. Third, a Supreme Court case called *Oneok v. Learjet*, considering the Natural Gas Act, emphasized that the ability of the federal government to regulate one particular area does not necessarily preclude state regulation in the same area. Other challenges around the ability of states and the federal government to regulate certain aspects of grid activities that have implications for DERs are working their way through federal courts. Although the mentioned cases have provided certainty in some respects, a general climate of uncertainty exists in states’ attempts to design new DER-centered regulations and programs.

<sup>24</sup> For example, PURPA’s Sections 1251, 1252, and 1254, and section 1254 of EPCRA 2005.





**FIGURE 2.10** Different ways in which the nature and scope of the future regulatory environment might evolve.

upon the standards developed by the Institute of Electrical and Electronics Engineers: IEEE Standard 1547 for Interconnecting Distributed Resources with Electric Power Systems, as they may be amended from time to time. In addition, agreements and procedures shall be established whereby the services offered shall promote current best practices of interconnection for distributed generation, including but not limited to practices stipulated in model codes adopted by associations of state regulatory agencies. All such agreements and procedures shall be just and reasonable and not unduly discriminatory or preferential.

While the legal justification under which federal jurisdiction might be further expanded is unclear, there is certainly a possibility that such justification might evolve over time.

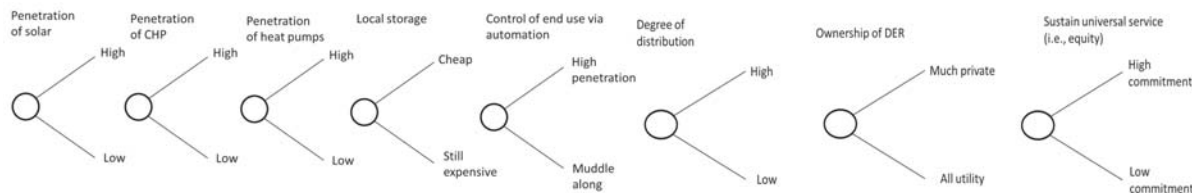
There is of course also the possibility that in some domains, local, state, or even regional regulatory responsibilities might be expanded. If larger differences develop among regulatory structures in different parts of the country, this could present a variety of complications. As pressure grows to adopt more innovative strategies to address resilience issues that impact large areas of interconnected systems, states and regions may decide they need to adopt more innovative approaches.

The possibility of greater grid defection by customers may result in those customers providing their own electricity, entirely removed from federal and state rate jurisdiction altogether. It is likely that this would occur only in situations

where the customer disconnects entirely from the grid. In such instances, states may have to address the terms and conditions under which customers may exit from or reenter the local distribution to assure (among other things) that legacy costs associated with utilities' planning to provide service to those customers are addressed, according to traditional cost-incurrence and equity principles of utility regulation.

### Penetration and Characteristics of Distributed Energy Resources

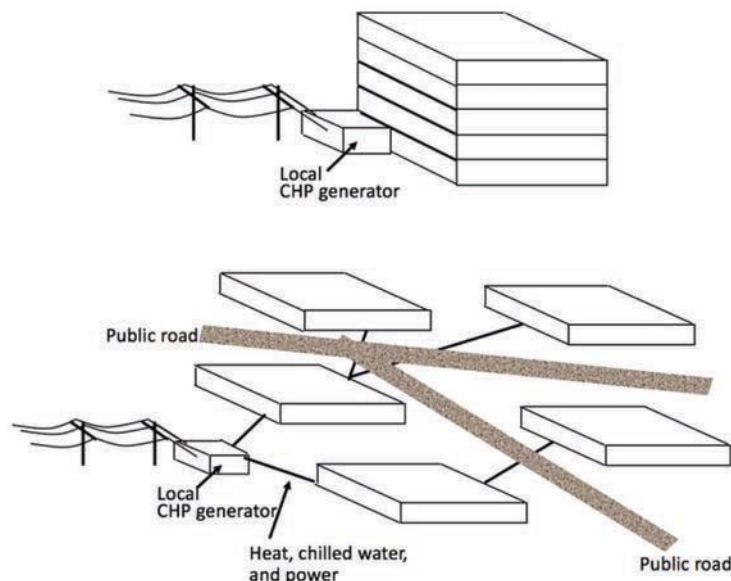
Closely linked to the way in which the future regulatory environment might evolve is the degree of penetration of distributed resources (Figure 2.11). The pace and extent of further deployment of DERs is the subject of major discussion in the industry. If the DOE SunShot targets are met, for example, rooftop solar will likely become cost competitive across much of the country without significant subsidies (Hagerman et al., 2016). Penetration of CHP has been much slower. Its future will depend in part on how the policy environment evolves and the wholesale-to-retail markup of natural gas. Costs are falling for local storage technology, but it is still only commercially viable in niche applications. Adoption could accelerate if costs fall and suppliers begin to offer storage with photovoltaic systems—with inverters and local intelligent control that reduces electricity bills and allows customers to continue to operate when grid power is unavailable.



**FIGURE 2.11** Different ways in which distributed resources might evolve in the future.

NOTE: CHP, combined heat and power; DER, distributed energy resource.





**FIGURE 2.12** Under most state laws, there is legal distinction between a utility that serves a multi-story building with its own distributed energy resource and combined heat and power, as shown at the top of this figure, and the situation in which the same loads are distributed across space and are served by a small microgrid. There is virtually no technical difference between these two situations. If laws were changed to allow private ownership of such microgrids (with equitable symmetric tariffs), future distribution systems could look very different. NOTE: CHP, combined heat and power.

There has been considerable discussion of smart controls for end-use devices, including the idea of “prices to devices” that would allow larger customers to decide when they will and will not operate particular electricity-using equipment given time-of-use pricing. While very extensive intelligent control is possible, what is less clear is when and whether the added hardware and intelligence will make economic sense.

### Legal Implementation of Non-Utility Microgrids

Today in most of the United States, state law grants exclusive service territories to legacy distribution utilities, although there are a few exceptions.<sup>25</sup> This means that with the exception of a customer selling power back to the local utility, only that utility can distribute power to another entity. It also means that only a traditional utility can move power across a public road or other public right-of-way. If state laws were changed in such a way as to allow small-scale microgrids (larger than a few MWs) to be operated by private

entities—with tariffs that symmetrically recognize the contributions of DERs while keeping the distribution company whole—the adoption of DERs could accelerate. Utility executives often argue that such a change would impose serious operational problems. However, from a technical point of view, there is very little difference between the two situations shown in Figure 2.12.

The committee asked several state regulatory agencies whether, in their jurisdictions, an entity other than the local distribution utility could build a small microgrid (e.g., less than a few 10s of MW), sell electric power to other entities, and be interconnected to the distribution utility. Several states noted that, as a matter of law, this was simply impossible in their states. Others indicated that the answer was more complex—an entity that wanted to engage in such activity would need to become a licensed and regulated utility. For example, staff of the Pennsylvania PUC said, “It is conceivable that an entity could perform such a function if they were properly licensed by the commission and the RTO and PJM. There may be some other legal factors that could limit their ability to sell power to entities other than the distribution utility and/or PJM Pennsylvania does allow net metering (see footnote 21) up to 3 MW.” Staff from the ICC noted, “Third parties that sell electric power to retail customers of an investor-owned utility must be licensed by the (ICC).” Staff of the New Hampshire Commission noted that in addition to having net metering, their state also has “group net metering (up to 1 MW).”

<sup>25</sup> New York is one exception where the state may grant multiple franchises to serve a particular location; however, it is then up to local municipalities to grant easements along public streets and roads in order for the utility to install necessary facilities. Some Pennsylvania communities have been granted multiple franchises resulting in different utilities’ distribution lines on opposite sides of the street with service drops to customers crossing overhead. Nonetheless, in most regions service franchises are granted exclusively to one provider.

## TODAY'S GRID AND THE EVOLVING SYSTEM OF THE FUTURE

For years, the regulatory framing under which electric power has been provided in the United States was built on a foundation of universal service—that is, that access to basic electric power is to some degree a right that all citizens should enjoy. Indeed, it was this belief that prompted the creation of the Rural Electrification Administration in 1935 to supply power across rural America to customers whose locations were too remote to be attractive to privately operated utilities.

Today, the technical capability exists to provide different levels of service to different customers. This raises policy questions about whether all customers deserve some basic level of reliable service on the grounds of equity. As discussed in Chapter 5 of this report, there are ways in which distribution systems that contain advanced automation and distributed generation could be “islanded” so as to provide some limited service in the event of a large-area, long-duration blackout of the bulk power system. How the incremental cost of such upgrades should be covered, and whether they should only be based on an end-use customer’s ability to pay, raises obvious issues of social equity.

Over time, there will likely be greater opportunities for customers to defect from the grid (i.e., provide all of their electricity needs with customer-owned generation and storage). The goal of ensuring that all customers have access to electricity service that is affordable and reliable, combined with society’s larger interest in assuring that a resilient electric system supports the availability of critical social services, suggests that policy makers should continue to pay close attention to this trend. Policy makers may need to pursue mechanisms that encourage grid integration as part of service and to ensure that grid defection does not adversely impact those customers who have no practical economic choice but to remain dependent on the electric system to serve their needs.

### Impacts of a Changing Climate

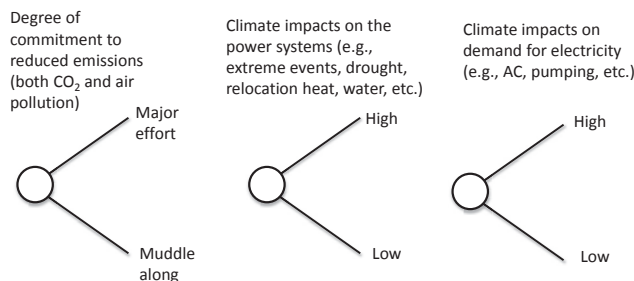
There remains uncertainty regarding how climate change and associated concerns will impact the electric power

system (Figure 2.13). While the impacts of climate change will unfold over the coming decades, policy choices made in the near future can have a profound impact on the extent of that change (White House, 2016). The changing climate will result in more frequent and more intense extreme events (Melillo et al., 2014) that will impose damage and other challenges on the power system. Higher ambient temperatures will create increased demand for system cooling. In some parts of the country, it will also bring deeper and more prolonged droughts that, in turn, will result in problems of securing sufficient water for system cooling unless traditional wet cooling is replaced with dry cooling. In some locations, such as coastal regions prone to rising sea levels and storm surge or inland locations prone to frequent wildfires or flooding, it may prove necessary to relocate some facilities. Climate change will likely also result in new demands for electric power including larger air conditioning loads and, in some locations, an increased demand for power to pump water.

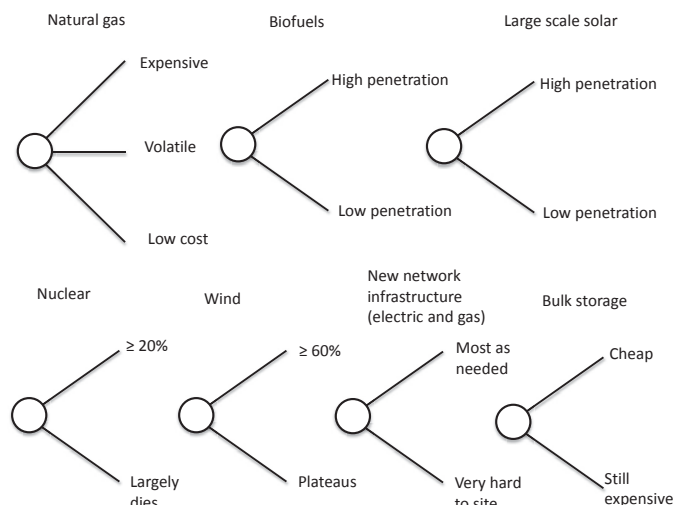
### Changes in the Sources of Bulk Power

The past few decades have seen dramatic shifts in the sources of bulk power employed in the United States, and uncertainty persists regarding the future (Figure 2.14). Natural gas has displaced generation at many coal-fired baseload power plants, and even existing nuclear plants are retiring before the end of their operating licenses. However, if prices once again become higher or more volatile, investors may shy away from putting capital into natural gas plants and the trend could be reversed, as it was in the past.

Many observers anticipate significant penetration of new renewables, especially wind, solar, and hydro power. Today, wind generation constitutes approximately 5 percent of total U.S. generation, but a number of analyses suggest that there is no technical reason why the nation could not generate more than 60 percent of its electricity from wind. However, achieving such a high level of penetration would impose considerable requirements on land use, both for siting the wind turbines and for constructing the necessary transmission infrastructure, much of which will need to cross state



**FIGURE 2.13** Climate change can affect, and be affected by, the power system.



**FIGURE 2.14** Possible change in the sources and nature of bulk power.

lines (MacDonald et al., 2016). Hence there is considerable uncertainty about the degree of future penetration of wind generation. Similar observations have been made with respect to solar generation. Many have argued that extensive use of biomass fuel, perhaps also with carbon capture and sequestration, will be necessary to achieve the objective of holding global warming to  $\leq 2^\circ\text{C}$ . At the same time, the widespread use of biomass imposes considerable logistical requirements and demands on land use (LaTourrette et al., 2011). Hence, it remains unclear how much future development will occur.

Nuclear power has contributed roughly 20 percent of the nation's electricity generation for the past few decades. Many forecasts of U.S. energy production continue to assume their continued contribution of roughly the same share of supply. With the cost pressures that nuclear plants are facing from inexpensive natural gas and subsidized renewables, and uncertainties about the cost and likelihood of life extension and relicensing, a number of plants have closed recently. New York state and Illinois recently adopted policies designed to keep existing plants operating (McGeehan, 2016). The only new plants under construction in the United States are in the service territory of vertically integrated utilities in the Southeast, where costs can be included in the rate base. In addition, the nation has largely abandoned aggressive research on more advanced reactor designs, so that for at least the next several decades the only options for new nuclear construction will likely be existing light-water reactor designs (DOE, 2017c; Ford et al., 2017). There may be some renewed interest in advanced reactor design research (DOE, 2017c), but the extent of programmatic support for this vision remains uncertain. Small modular reactors have received a lot of attention in part because they require less capital investment and offer much greater siting flexibility. Despite these benefits, however, long-standing efforts have

never reached commercial construction (Larson, 2016). Investment in new, small, and advanced reactors may require a number of changes in business models and reactor designs that allow standardized and quicker manufacturing of components and construction of reactors.

Today, technologies for cost-effective bulk storage are limited. Pumped hydro storage imposes considerable land use and other environmental costs, and only a few facilities for compressed air storage have been built. Battery storage is beginning to have some impact on the power system, especially in behind-the-meter applications. In 2012, DOE established the Joint Center for Energy Storage Research (JCESR) as one of its "Energy Innovation Hubs." JCESR's stated goal is to "deliver electrical energy storage with five times the energy density and one-fifth the cost" of present storage technologies (Crabtree, 2016). In addition to striving to develop batteries that would allow all electric passenger vehicles to be profitably marketed at a cost of approximately \$20,000 and with a range of 200 miles, JCESR director George Crabtree has articulated remarkably aggressive goals for affordable grid storage, including battery technology that would be competitive with pumped hydro storage, chemically based, and capable of seasonal storage. However, battery experts with whom the committee discussed the JCESR goals for bulk grid storage have expressed considerable doubt about achieving those goals, especially on the time scale of the next several decades.

Nonetheless, all electric vehicles with those capabilities would have an impact on both the transportation sector and on electricity demand. Whether or not the JCESR goals are met, a much higher penetration of electric or hybrid vehicles may well occur on the time scale of the next several decades. With greater adoption of electric and plug-in hybrid vehicles, there may be greater opportunities for using connected vehicle batteries to improve grid resilience—for example,

by using electric vehicle batteries to provide a fraction of a home's electricity demand during a large-area, long-duration outage (see Chapter 5).

## SUSTAINING AND IMPROVING THE RESILIENCE OF A GRID THAT IS CHANGING RAPIDLY AND IN UNCERTAIN WAYS

From all of the foregoing, five things are apparent:

1. The grid is undergoing dramatic change. This will be especially true over the next few years at the distribution level where DERs continue to increase and change the relationship of utilities to end users. While DERs may provide many opportunities to increase grid resilience, this will require regulatory changes and effective planning and coordination. Over the next decade or two, major changes are also likely in bulk power transmission.
2. Much of the hardware that makes up the grid is long lived, which limits the rate of change in the industry. However, over periods of a decade or two, many changes are possible, and it is virtually impossible to know how the future grid will evolve.
3. No single entity is in charge of planning the evolution of the grid. That will become ever more true as more and more players become involved, particularly regarding deployment and operation of DERs at the distribution level.
4. All players will be concerned about reliability, both for themselves and collectively. Only a few are likely to be focused in a serious way on identifying growing system-wide vulnerabilities or identifying changes needed to assure resilience.
5. Today, virtually no one has a primary mission of building and sustaining increased system-wide resilience or developing strategies to cover the cost of investments to increase resilience in the face of low probability events that could have very large economic and broader social consequences.

These five observations carry profound implications for the future resilience of the power system. In Chapter 3, the committee explores the many types of events that can give rise to large-area, long-duration outages. Chapters 4, 5, and 6 correspond to the three stages of the resilience framework illustrated in Figure 1.2, making specific recommendations in the course of the discussion. Finally, in Chapter 7 the committee both summarizes those recommendations and comes back to the broader implications of the five observations above to consider an integrated perspective to the issue of electricity system resilience and how best to assure that continued attention is directed at building and sustaining system-wide resilience of the nation's power system.

## REFERENCES

- ACEEE (American Council for an Energy-Efficient Economy). 2012. *Financial Incentives for Energy Efficiency Retrofits in Buildings*. Summer Study on Energy Efficiency in Buildings, Pacific Grove, Calif., August 12–17. <http://aceee.org/files/proceedings/2012/data/papers/0193-000422.pdf>.
- AEE (Advanced Energy Economy). 2015. "Can Utilities Get Smarter with Smart Meters." <http://blog.aee.net/can-utilities-get-smarter-with-smart-meters>. Accessed July 11, 2017.
- Alliance to Save Energy. 2013. *The History of Energy Efficiency*. Alliance Commission on National Energy Efficiency Policy, Washington, D.C., January. [https://www.ase.org/sites/ase.org/files/resources/Media%20browser/ee\\_commission\\_history\\_report\\_2-1-13.pdf](https://www.ase.org/sites/ase.org/files/resources/Media%20browser/ee_commission_history_report_2-1-13.pdf).
- APPA (American Public Power Association). 2014. *Evaluation of Data Submitted in APPA's 2013 Distribution System Reliability & Operations Survey*. [http://www.publicpower.org/files/PDFs/2013DSReliabilityAndOperationsReport\\_FINAL.pdf](http://www.publicpower.org/files/PDFs/2013DSReliabilityAndOperationsReport_FINAL.pdf).
- Bakke, G. 2016. *The Grid: The Fraying Wires Between Americans and Our Energy Future*. New York: Bloomsbury Press.
- Blumsack, S., L. Lave, and J. Apt. 2008. "Electricity Prices and Costs under Regulation and Restructuring." Paper presented at the 2008 Industry Studies Annual Conference, Boston, Mass., May 1–2. [http://web.mit.edu/is08/pdf/Blumsack\\_Lave\\_Apt%20Sloan%20paper.pdf](http://web.mit.edu/is08/pdf/Blumsack_Lave_Apt%20Sloan%20paper.pdf).
- BNEF (Bloomberg New Energy Finance). 2016. "Reactors in the Red: Financial Health of the U.S. Nuclear Fleet." <http://docplayer.net/26060517-Reactors-in-the-red-financial-health-of-the-us-nuclear-fleet.html>. Accessed June 28, 2017.
- BPA (Bonneville Power Administration). 2017. "Facts and figures." <https://www.bpa.gov/news/pubs/generalpublications/gi-bpa-facts.pdf>.
- CAISO (California Independent System Operator). 2017. "Western Energy Imbalance Market (EIM)." <https://www.caiso.com/informed/Pages/EIMOverview/Default.aspx>. Accessed July 13, 2017.
- CARB (California Air Resources Board). 2014. "Assembly Bill 32 Overview." <https://www.arb.ca.gov/cc/ab32/ab32.htm>. Accessed September 21, 2016.
- Crabtree, G. 2016. *Storage at the Threshold: Beyond Lithium-ion Batteries*. [http://renewableenergy.illinoisstate.edu/downloads/speaker-presentations/2016\\_energy\\_storage/2%20George%20Crabtree.pdf](http://renewableenergy.illinoisstate.edu/downloads/speaker-presentations/2016_energy_storage/2%20George%20Crabtree.pdf).
- De Martini, P., and L. Kristov. 2015. *Distribution Systems in a High Distributed Energy Resources Future*. Future Electric Utility Regulation Report No. 2, Lawrence Berkeley National Laboratory, October. [https://emp.lbl.gov/sites/all/files/FEUR\\_2%20distribution%20systems%2020151023.pdf](https://emp.lbl.gov/sites/all/files/FEUR_2%20distribution%20systems%2020151023.pdf).
- DOE (Department of Energy). 2015. "Modernizing the Electric Grid." *Quadrennial Energy Review First Installment: Transforming U.S. Energy Infrastructures in a Time of Rapid Change*. <http://energy.gov/epsa/downloads/quadrennial-energy-review-first-installment>. Accessed July 13, 2017.
- DOE. 2016a. "North American Electric Reliability Corporation Interconnections." [https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NERC\\_Interconnection\\_1A.pdf](https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NERC_Interconnection_1A.pdf).
- DOE. 2016b. "Residential Renewable Energy Tax Credit." <http://energy.gov/savings/residential-renewable-energy-tax-credit>. Accessed September 22, 2016.
- DOE. 2017a. *Quadrennial Energy Review: Transforming the Nation's Electricity System: The Second Installment of the QER*. January 2017. <https://energy.gov/epsa/downloads/quadrennial-energy-review-second-installment>. Accessed July 13, 2017.
- DOE. 2017b. *Modern Distribution Grid Vol. II: Advanced Technology Maturity Assessment*. [http://doe-dspx.org/wp-content/uploads/2017/03/Modern-Distribution-Grid\\_Volume-II\\_v1.1\\_03272017.pdf](http://doe-dspx.org/wp-content/uploads/2017/03/Modern-Distribution-Grid_Volume-II_v1.1_03272017.pdf).
- DOE. 2017c. *Vision and Strategy for the Development and Deployment of Advanced Reactors*. <https://energy.gov/sites/prod/files/2017/02/f34/71160%20VISION%20%20STRATEGY%202017%20FINAL.pdf>.



- DSIRE (Database of State Incentives for Renewables and Efficiency). 2016a. "Renewable Portfolio Standard Policies." <http://www.dsireusa.org/resources/detailed-summary-maps/>. Accessed July 13, 2017.
- DSIRE. 2016b. "3rd Party Solar PV Power Purchase Agreement (PPA)." <http://ncsolarcen-prod.s3.amazonaws.com/wp-content/uploads/2014/11/3rd-Party-PPA.pdf>.
- DSIRE. 2016c. "Net Metering." [http://ncsolarcen-prod.s3.amazonaws.com/wp-content/uploads/2016/07/Net\\_Metering1.pdf](http://ncsolarcen-prod.s3.amazonaws.com/wp-content/uploads/2016/07/Net_Metering1.pdf).
- DSIRE. 2016d. "Find Policies & Incentives by State." <http://www.dsireusa.org/>. Accessed September 22, 2016.
- EEl (Edison Electric Institute). 2017. "Industry Capital Expenditures." [http://www.eei.org/resourcesandmedia/industrydataanalysis/industryfinancialanalysis/QtrlyFinancialUpdates/Documents/EEI\\_Industry\\_Capex\\_Functional\\_2017.04.21.pptx](http://www.eei.org/resourcesandmedia/industrydataanalysis/industryfinancialanalysis/QtrlyFinancialUpdates/Documents/EEI_Industry_Capex_Functional_2017.04.21.pptx). Accessed July 13, 2017.
- EIA (Energy Information Administration). 2010. "Electricity: Status of Electricity Restructuring by State." [http://www.eia.gov/electricity/policies/restructuring/restructure\\_elect.html](http://www.eia.gov/electricity/policies/restructuring/restructure_elect.html). Accessed September 22, 2016.
- EIA. 2015. "What is U.S. Electricity by Generation Source?" <https://www.eia.gov/tools/faqs/faq.cfm?id=427&t=3>. Accessed September 22, 2016.
- EIA. 2016a. Electric Power Sales, Revenue, and Energy Efficiency. Form EIA-861, Detailed Data Files. <https://www.eia.gov/electricity/data/eia861/>. Accessed July 13, 2017.
- EIA. 2016b. *Monthly Energy Review*. <https://www.eia.gov/totalenergy/data/monthly/pdf/mer.pdf>.
- EIA. 2016c. "Preliminary Monthly Electric Generator Inventory." <http://www.eia.gov/electricity/data/eia860m/>. Accessed July 13, 2017.
- EIA. 2016d. "Today in Energy: Demand Trends, Prices, and Policies Drive Recent Electric Generation Capacity Additions." <http://www.eia.gov/todayinenergy/detail.cfm?id=25432>. Accessed September 20, 2016.
- EIA. 2016e. "Today in Energy: Solar, Natural Gas, Wind Make Up Most 2016 Generation Additions." <http://www.eia.gov/todayinenergy/detail.php?id=29212>. Accessed December 19, 2016.
- EPRI (Electric Power Research Institute). 2011. *Needed: A Grid Operating System to Facilitate Grid Transformation*. [https://www.smartgrid.gov/files/Needed\\_Grid\\_Operating\\_System\\_to\\_Facilitate\\_Grid\\_Transformati\\_201108.pdf](https://www.smartgrid.gov/files/Needed_Grid_Operating_System_to_Facilitate_Grid_Transformati_201108.pdf).
- EPRI. 2015. *The Integrated Grid: A Benefit-Cost Framework*. Final Report, 3002004878. Palo Alto, Calif.: EPRI.
- FERC (Federal Energy Regulatory Commission). 2016a. "Regional Transmission Organizations (RTO)/Independent System Operators (ISO)." <https://www.ferc.gov/industries/electric/indus-act/rto.asp>. Accessed July 13, 2017.
- FERC. 2016b. *Assessment of Demand Response and Advanced Metering*. <https://www.ferc.gov/legal/staff-reports/2016/DR-AM-Report2016.pdf>.
- Ford, M.J., A. Abdulla, M.G. Morgan, and D.G. Victor. 2017. Expert assessments of the state of U.S. advanced fission innovation. *Energy Policy* 108: 194–200.
- Glass, J. 2016. "Enhancing the Resiliency of the Nation's Electric Power Transmission and Distribution System," presentation to the Committee on Enhancing the Resilience of the Nation's Electric Power Transmission and Distribution System, September 29, Washington, D.C.
- GMLC (Grid Modernization Laboratory Consortium). 2017. *Grid Modernization: Metrics Analysis*. Richland, Wash.: Pacific Northwest National Laboratory.
- Gridwise Alliance. 2016. "3rd Annual Grid Modernization Index." [http://www.gridwise.org/report\\_download.asp?id=17](http://www.gridwise.org/report_download.asp?id=17). Accessed July 13, 2017.
- Hagerman, S., P. Jaramillo, and M.G. Morgan. 2016. Is rooftop solar PV at socket parity without subsidies? *Energy Policy* 89: 84–94.
- Hirschman, A. 1970. *Exit, Voice and Loyalty: Responses to Decline in Firms, Organizations and States*. Cambridge: Harvard University Press.
- Hoovers. 2017. "Arizona Public Service Company Revenue and Financial Data." [http://www.hoovers.com/company-information/cs/revenuefinancial.arizona\\_public\\_service\\_company.959a800ac6670f2a.html](http://www.hoovers.com/company-information/cs/revenuefinancial.arizona_public_service_company.959a800ac6670f2a.html). Accessed February 10, 2017.
- IEEE (Institute of Electrical and Electronics Engineers). 2013. *Standard for Interconnecting Distributed Resources with Electric Power Systems*. [http://grouper.ieee.org/groups/scc21/1547/1547\\_index.html](http://grouper.ieee.org/groups/scc21/1547/1547_index.html). Accessed July 13, 2017.
- IRC (ISO/RTO Council). 2015. "Members at a Glance." <http://www.isorto.org/About/Members/allmembers>. Accessed December 18, 2016.
- Karlin, B. 2012. *Public Acceptance of Smart Meters: Integrating Psychology and Practice*. ACEEE Summer Study on Energy Efficiency in Buildings. <http://aceee.org/files/proceedings/2012/data/papers/0193-000243.pdf>.
- Keogh, M., and C. Cody. 2013. *Resilience in Regulated Utilities*. National Association of Regulatory Utility Commissioners' Grants and Research Department, November. <https://pubs.naruc.org/pub/536F07E4-2354-D714-5153-7A80198A436D>. Accessed July 13, 2017.
- Kwasinski, A. 2016. Quantitative model and metrics of electric grids' resilience evaluated at a power distribution level. *Energies* 9(93).
- Larson, A. 2016. "Is There a Market for Small Modular Reactors?" *Power Magazine*, June 1. <http://www.powermag.com/market-small-modular-reactors/>. Accessed July 13, 2017.
- LaTourrette, T., D.S. Ortiz, I. Hlavka, N. Burger, and G. Cecchine. 2011. *Supplying Biomass to Power Plants: A Model of the Costs of Utilizing Agricultural Biomass in Cofired Power Plants*. Santa Monica, Calif.: Rand Corporation. [http://www.rand.org/content/dam/rand/pubs/technical\\_reports/2011/RAND\\_TR876.pdf](http://www.rand.org/content/dam/rand/pubs/technical_reports/2011/RAND_TR876.pdf).
- Lave, L.B., J. Apt, and S. Blumsack. 2004. Rethinking electricity deregulation. *The Electricity Journal* 17(8): 11–26.
- Lazard. 2015. *Lazard's Levelized Cost of Energy Analysis—Version 9.0*. <https://www.lazard.com/media/2390/lazards-levelized-cost-of-energy-analysis-90.pdf>.
- MacDonald, A.E., C.T. Clack, A. Alexander, A. Dunbar, J. Wilczak, and Y. Xie. 2016. Future cost-competitive electricity systems and their impact on US CO<sub>2</sub> emissions. *Nature Climate Change* 6: 526–531.
- McAnany, J. 2017. *2016 Demand Response Operations Market Activities Report*. <http://www.pjm.com/~media/markets-ops/dsr/2016-demand-response-activity-report.aspx>. Accessed July 13, 2017.
- McGeehan, P. 2016. "New York State Aiding Nuclear Plants with Millions in Subsidies" *New York Times*, August 1. [http://www.nytimes.com/2016/08/02/nyregion/new-york-state-aiding-nuclear-plants-with-millions-in-subsidies.html?\\_r=0](http://www.nytimes.com/2016/08/02/nyregion/new-york-state-aiding-nuclear-plants-with-millions-in-subsidies.html?_r=0). Accessed January 2, 2017.
- Melillo, J.M., T.C. Richmond, and G.W. Yohe. 2014. *Climate Change Impacts in the United States: The Third National Climate Assessment*. U.S. Global Change Research Program. doi:10.7930/J0Z31WJ2.
- MIT (Massachusetts Institute of Technology). 2011. *The Future of the Electric Grid*. <http://energy.mit.edu/wp-content/uploads/2011/12/MITEI-The-Future-of-the-Electric-Grid.pdf>.
- MIT. 2016. *Utility of the Future: An MIT Energy Initiative Response to an Industry in Transition*. <http://energy.mit.edu/wp-content/uploads/2016/12/Utility-of-the-Future-Full-Report.pdf>.
- NAE (National Academy of Engineering). 2003. "Greatest Engineering Achievements of the 20th Century." <http://www.greatachievements.org/>. Accessed September 22, 2016.
- NASEM (National Academies of Sciences, Engineering, and Medicine). 2016. *The Power of Change: Innovation for Development and Deployment of Increasingly Clean Electric Power Technologies*. Washington, D.C.: The National Academies Press.
- Navigant Research. 2013. *The Lithium Ion Battery Market*. [https://www.arpa-e.energy.gov/sites/default/files/documents/files/Jaffe\\_RANGE\\_Kickoff\\_2014.pdf](https://www.arpa-e.energy.gov/sites/default/files/documents/files/Jaffe_RANGE_Kickoff_2014.pdf).
- NERC (North American Electric Reliability Corporation). 2010. "Functional Model." <http://www.nerc.com/pa/Stand/Pages/FunctionalModel.aspx>. Accessed September 22, 2016.
- NERC. 2011. *Special Report: Spare Equipment Database System*. Atlanta: NERC.
- NERC. 2014. *NERC CIP-014 Physical Security Standards*. <http://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-1.pdf>.
- NERC. 2016a. *Glossary of Terms Used in NERC Reliability Standards*. [http://www.nerc.com/files/glossary\\_of\\_terms.pdf](http://www.nerc.com/files/glossary_of_terms.pdf).



- NERC. 2016b. *Distributed Energy Resources: Connection, Modeling and Reliability Considerations*. <http://www.nerc.com/comm/Other/essntlrbltysrvckskfrDL/May%202016%20Meeting%20Materials.pdf>.
- NERC. 2017. "Critical Infrastructure Protection Compliance." <http://www.nerc.com/pa/CI/Comp/Pages/default.aspx>. Access March 13, 2017.
- NJBPU (New Jersey Board of Public Utilities). 2015. *Record of Decision*, May 21. <http://www.state.nj.us/bpu/pdf/boardorders/2014/20140521/5-21-14-2I.pdf>.
- NJBPU. 2017. In the Matter of the Petition of Rockland Electric Company for Approval of an Advanced Metering Program; and for Other Relief. BPU Docket No. ER16060524. [http://www.nj.gov/rpa/docs/ER16060524\\_Rate\\_Counsel\\_Initial\\_Brief\\_Rockland\\_AMI.pdf](http://www.nj.gov/rpa/docs/ER16060524_Rate_Counsel_Initial_Brief_Rockland_AMI.pdf). Accessed July 13, 2017.
- NRC (National Research Council). 2012. *Terrorism and the Electric Power Delivery System*. Washington, D.C.: The National Academies Press.
- Parfomak, P.W. 2014. *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*. <https://fas.org/sgp/crs/homesecl/R43604.pdf>.
- PJM. 2016. *Load Forecast Report*, January. <http://www.pjm.com/~media/documents/reports/2016-load-report.ashx>. Accessed September 21, 2016.
- PJM. 2017. "Fact at a Glance." <https://www.pjm.com/~media/about-pjm/newsroom/fact-sheets/pjm-at-a-glance.ashx>. Accessed February 20, 2017.
- Platts. 2014. "Utility Service Territories of North America." <http://www.platts.com/products/utility-service-territories-north-america-map>. Accessed July 13, 2017.
- Plug-in America. 2016. "State and Federal Incentives." <https://pluginamerica.org/why-go-plug-in/state-federal-incentives/>. Accessed September 21, 2016.
- PNNL (Pacific Northwest National Laboratory). 2015. *The Emerging Interdependence of the Electric Power Grid & Information and Communication Technology*. PNNL-24643, August. [http://www.pnnl.gov/main/publications/external/technical\\_reports/PNNL-24643.pdf](http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24643.pdf).
- Reuters. 2010. "Smart Grid Skepticism Derails Baltimore Plan." <http://blogs.reuters.com/great-debate/2010/06/23/smart-grid-scepticism-derails-baltimore-plan/>. Accessed July 13, 2017.
- RGGI (Regional Greenhouse Gas Initiative). 2016. "CO<sub>2</sub> Auctions, Tracking & Offsets." <https://www.rggi.org/market>. Accessed September 21, 2016.
- SNL (Sandia National Laboratories). 2014. *Conceptual Framework for Developing Resilience Metrics for the Electricity, Oil, and Gas Sectors in the United States*. <https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/EnergyResilienceReportSAND2014-18019o.pdf>.
- SoCo (Southern Company). 2017. "Overview of Our Business." <http://www.southerncompany.com/about-us/our-business/home.cshtml#>. Accessed February 20, 2017.
- Spence, A., C. Demski, C. Butler, K. Parkhill, and N. Pidgeon. 2015. Public perceptions of demand-side management and a smarter energy future. *Nature Climate Change* 5: 550–554.
- State of New York. 2014. *Reforming the Energy Vision: NYS Department of Public Service Staff Report and Proposal*. CASE 14-M-0101. <http://www3.dps.ny.gov/W/PSCWeb.nsf/All/C12C0A18F55877E785257E6F005D533E?OpenDocument>. Accessed September 21, 2016.
- TCR (Tabors Caramanis Rudkevich). 2016. "Developing Competitive Electricity Markets and Pricing Structures." White paper prepared for New York State Energy Research and Development Authority and New York State Department of Public Service, Contract 64271. <https://www.hks.harvard.edu/hepg/Papers/2016/TCR.%20White%20Paper%20on%20Developing%20Competitive%20Electricity%20Markets%20and%20Pricing%20Structures.pdf>.
- Tierney, S. 2016a. *The U.S. Coal Industry: Challenging Transitions in the 21st Century*. <http://www.analysisgroup.com/uploadedfiles/content/insights/publishing/tierney%20-%20coal%20industry%20-%2021st%20century%20challenges%209-26-2016.pdf>.
- Tierney, S. 2016b. *The Value of "DER" to "D": The Role of Distributed Energy Resources in Supporting Local Electric Distribution System Reliability*. [http://www.cpuc.ca.gov/uploadedFiles/CPUC\\_PublicWebsite/Content/About\\_Us/Organization/Divisions/Policy\\_and\\_Planning/Thought\\_Leaders\\_Events/Tierney%20White%20Paper%20-%20Value%20of%20DER%20to%20D%20-%202016%20FINAL.pdf](http://www.cpuc.ca.gov/uploadedFiles/CPUC_PublicWebsite/Content/About_Us/Organization/Divisions/Policy_and_Planning/Thought_Leaders_Events/Tierney%20White%20Paper%20-%20Value%20of%20DER%20to%20D%20-%202016%20FINAL.pdf).
- USCB (U.S. Census Bureau). 2016. "QuickFacts." <http://www.census.gov/quickfacts/>. Accessed December 18, 2016.
- USDA (U.S. Department of Agriculture). 2016. "Rural Utilities Service." <https://www.rd.usda.gov/about-rd/agencies/rural-utilities-service>. Accessed July 13, 2017.
- White House. 2016. *Opportunities to Enhance the Nation's Resilience to Climate Change*. <https://www.whitehouse.gov/sites/default/files/finalresilienceopportunitiesreport.pdf>.
- Willis, H.H., and K. Loa. 2015. *Measuring the Resilience of Energy Distribution Systems*. Santa Monica, Calif.: RAND Corporation.

# 3

## The Many Causes of Grid Failure

### INTRODUCTION

A wide variety of events can cause disruption of the power system. As noted in Chapter 1, given the numerous and diverse potential sources of disruption, it is impressive that relatively few large-area, long-duration outages have occurred. The causes of outages differ in a number of important ways. Two of the most important differences are as follows: (1) how much warning system operators have that a disruption is coming so they can take protective action, and (2) how much of the physical and cyber control systems that make up the power system remain operative once the disruption has passed. Figure 3.1 categorizes disruptions by the amount of advance warning that operators and others are likely to receive and the amount of time it takes to recover. Figure 3.2 categorizes the range of damages that may result after a disruption occurs.

### DIFFERENT CAUSES REQUIRE DIFFERENT PREPARATION AND HAVE DIFFERENT CONSEQUENCES

Building a strategy to increase system resilience requires an understanding of a wide range of preparatory, preventative, and remedial actions and an awareness of how these actions impact planning, operation, and restoration over the entire life cycle of different kinds of grid failures. Strategies must be crafted with awareness and understanding of the temporal arc of a major outage, as well as how this differs from one type of event to another.

It is also important to differentiate between actions designed to make the grid more robust and resilient to failure (e.g., wind resistant steel or concrete poles rather than wood poles; opaque fences around substations to protect against damage from firearms) and those that improve the effectiveness of recovery (e.g., preemptive powering down of select pieces of the system to minimize damage). Some actions serve both strategies, some serve one but not the other, and some serve one while inhibiting the other. For example, good substation design with clear separation of functions makes

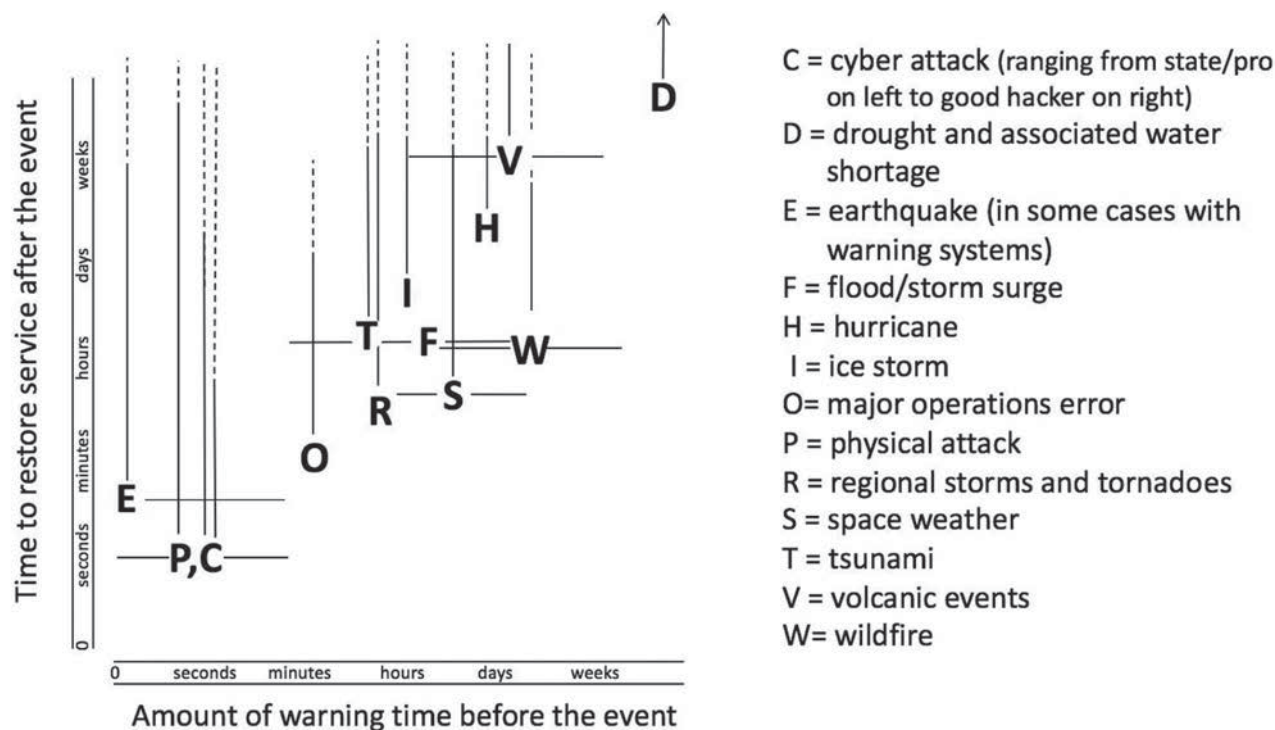
the substation more resistant to damage and helps repair crews. Building a coffer dam around a transformer may make it more resistant to flooding, but by limiting access for heavy equipment it can also make it harder to complete repairs when it actually fails. Of course a coffer dam does nothing to guard against the effects of earthquake or cyber attack. Similarly, concrete poles may be more resistant to wind but offer no clear advantage or disadvantage in restoration.

The timing of repairs is different depending on the cause. For example, repairs can begin immediately after a tornado has passed, but flooding following a hurricane can delay the start of repairs for weeks and impede restoration efforts. Good planning and preparation are essential to mitigating, ameliorating, and recovering from major outages effectively. Systems—both human and technical—must be built prior to grid failure to allow the responders to assess the extent of failure and damage, dispatch resources effectively, and draw on established component inventories, supply chains, crews, and communications. The next section reviews the major causes of outages depicted in Figure 3.1, beginning with those for which operators have the least warning and ending with those for which they have the most. The chapter then makes a number of general findings and recommendations related to both human and natural threats to the power system.

### REVIEWING THE CAUSES OF OUTAGES

#### Earthquake

Moving through Figure 3.1 from left to right, the first point is labeled E for earthquake. Especially in the West, the central Mississippi valley, the coastal area of South Carolina, and southern Alaska and Hawaii (Figure 3.3), the potential for disruption of major power system equipment by earthquake is significant. Severe damage to distribution poles, transmission towers, and substations can result. Generators may be damaged or subjected to enough stress that they have to be taken off-line. For example, the North Anna Nuclear Power Station was taken off-line following a magnitude 5.8



**FIGURE 3.1** Mapping of events that can cause disruption of power systems. The horizontal placement provides some indication of how much warning time there may be before the event. The vertical axis provides some indication of how long it may take to recover after the event. Lines provide a representation of variability in these estimates.

earthquake in Virginia in 2011 and remained off-line for more than 10 weeks as the owner and operator conducted thorough damage assessments and the Nuclear Regulatory Commission granted approval for restart (Vastag, 2011; Pelletier, 2012). In addition, there is substantial risk of the loss of fuel, particularly from natural gas systems, given the long supply chain and vulnerability of pipelines to earthquakes.

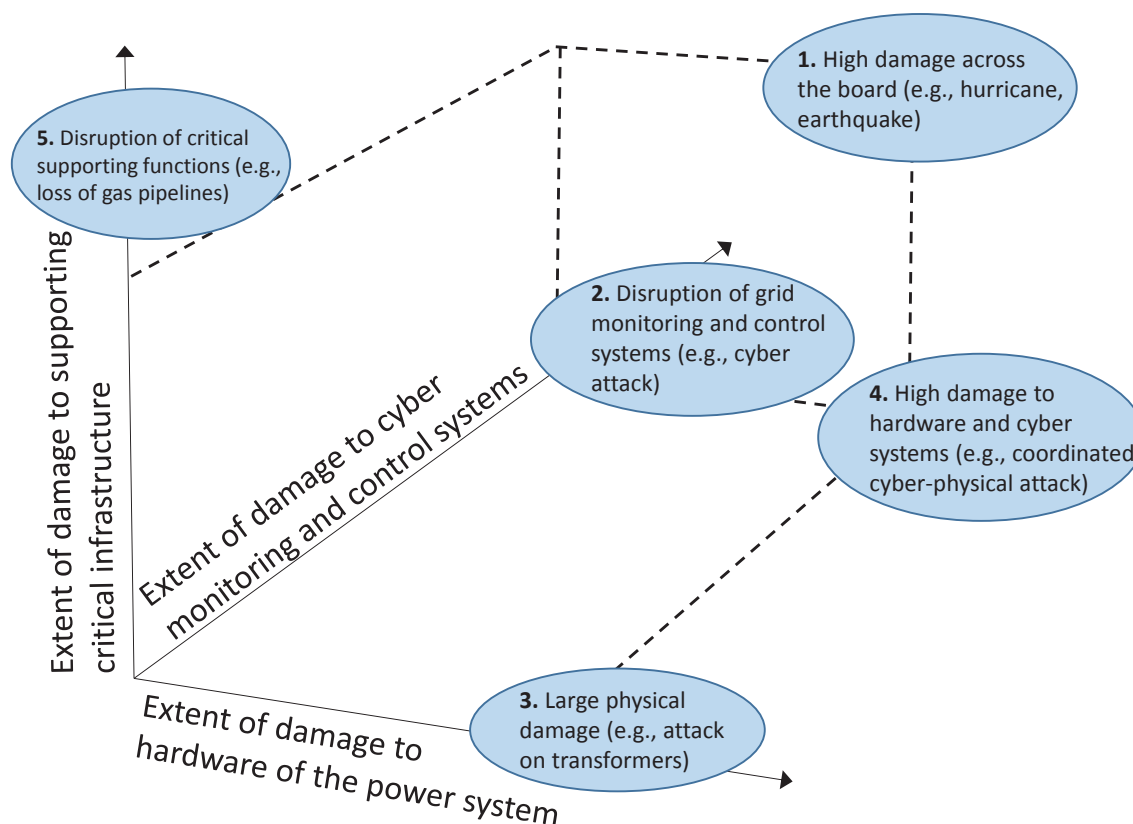
While earthquakes typically come without warning, the propagation velocity of earthquake waves is much slower than the speed of light, so that in some cases it is possible with appropriate instrumentation to obtain several seconds of advance warning (hence the horizontal line that runs to the right of point E in Figure 3.1). When possible, such warning could give time to de-energize critical components so as to minimize damage. Research is continuing on a wide range of grid-specific technologies. Organizations like the Pacific Earthquake Engineering Center are working on technologies such as more durable ceramic and non-ceramic insulators, flexible electrical connectors, and advanced materials for towers and attachments. Restoration following a major earthquake is a massive problem requiring a wide range of difficult engineering and construction projects in a compromised environment, with competition from other restoration priorities. For example, key bridges or roads required to access damaged facilities may be impassable. If an earthquake destroys key generating, substation, or transmission equipment, it may take weeks or months to restore service.

### Physical Attack

A physical attack, denoted by point P, could occur without warning or with only limited warning. Physical attacks on major system components could cause serious physical damage, especially to large transformers and other hard to replace substation and transmission equipment such as high-voltage circuit breakers. The possibility of such attacks has been a concern for many years (OTA, 1990; NRC, 2012; DOE, 2015; Parfomak, 2014). Globally, transmission and distribution systems have been a focus of physical attacks, bombings, and terrorist activity—for example, in Afghanistan, Colombia, Iraq, Peru, and Thailand (NRC, 2012). In the United States, there have been relatively few well-planned attacks on the electricity system, though the 2013 sniper attack of the Metcalf transmission substation (Box 3.1) provides a reminder of the physical vulnerability of the system. Recovery could easily require many days or weeks. Generation facilities tend to have greater physical security and thus are less vulnerable to physical attack than substation and transmission facilities.

### Cyber Attack

Like a physical attack, a cyber attack, denoted with a C, could also occur with limited or no warning. The best defense against cyber attacks is preventing intrusions to



**FIGURE 3.2** Illustration of distinct types of damages that can affect power systems. Major disruptive events such as hurricanes or earthquakes can cause damage across the board—to the physical and cyber components of the power system and supporting critical infrastructure (case 1). While it is possible to do physical damage with a cyber attack, many cyber attacks would not give rise to physical damage but could cause considerable disruption in the ability to monitor and control the power system (case 2). In contrast, a terrorist attack on high-voltage transformers could result in extensive damage to critically important hardware while leaving monitoring and control capabilities intact (case 3). A coordinated cyber-physical attack can simultaneously cause serious physical damage to grid components and impede operators' ability to monitor and control the grid (case 4). Loss of other infrastructure such as natural gas pipelines or communication systems can have impacts on the ability of the system to operate (case 5).

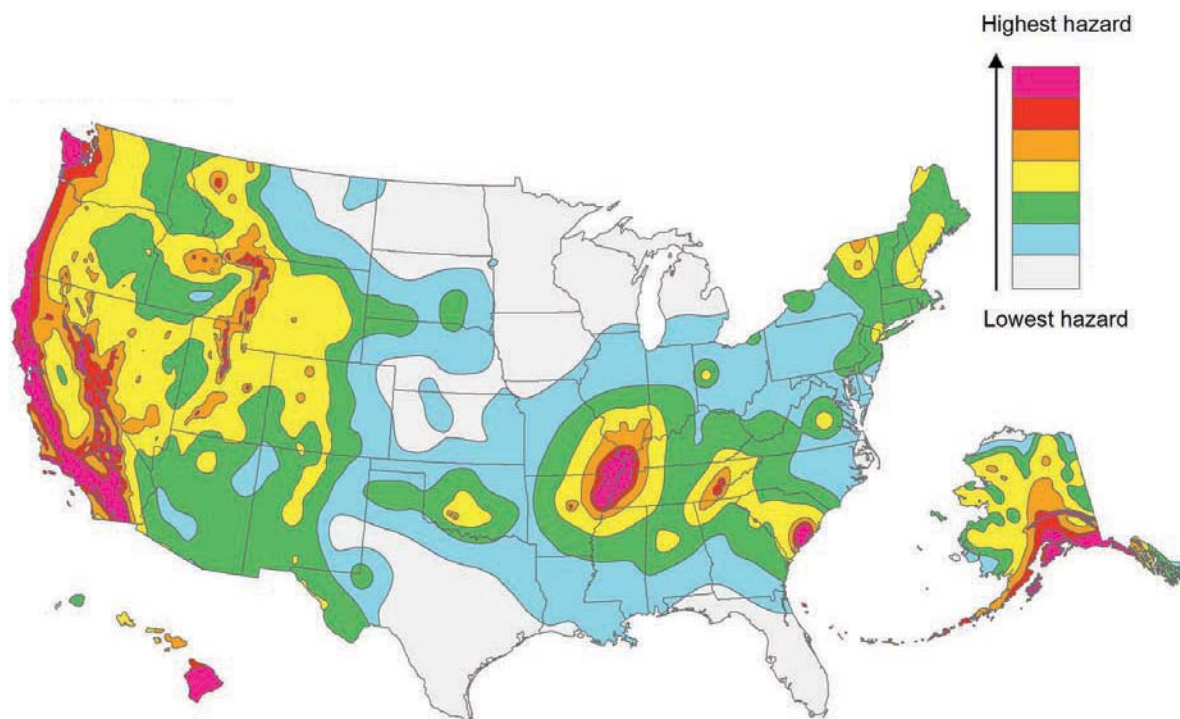
critical systems and detecting and expunging malware before it becomes activated. However, if that is not possible, the consequences of a successful cyber attack may be almost instantaneous, they could take a few seconds to some minutes to be fully realized, or an attacker may lay dormant for months collecting information as happened in the 2015 cyber attack on the Ukrainian power system (Box 3.2). It is difficult to determine how many cyber attacks have been attempted against U.S. utilities, by what means, and with what consequences.

In the time between detection of an intrusion and manifestation of any consequences, it may be possible to take some steps to limit the potential disruptive impacts. In many cases a cyber attack may not give rise to major physical damage to the system, although in some circumstances physical damage can result, especially if the attackers are sophisticated. Depending on the nature of the attack, just how long it would take to restore is unclear. The unique issues associated with

cyber risks and restoration are discussed in Chapters 4 and 6. There are also diverse types of cyber attacks and vulnerabilities within the electricity system. According to recent analysis done for the Quadrennial Energy Review (Argonne National Laboratory et al., 2016), the electricity system vulnerabilities include the following:

- *Supervisory control and data acquisition systems* that rely on modern communication infrastructure to collect data and send control signals in both the bulk power system (generation and transmission) and at the substation level;
- *Large power plant distributed control systems* that use local communications channels to perform local control on large power plants;
- *Smart grid technologies*, including software-based components with communication capabilities, used to increase the reliability, security, and efficiency of





**FIGURE 3.3** U.S. Geological Survey assessment of earthquake hazard across the United States.  
SOURCE: Petersen et al. (2014).

the grid as well as communicate data between utilities and customers;

- *Distributed energy resources* that are connected to open networks for communication and can include smart inverters with remote access;
- *Supply chain* that might have vulnerabilities of legacy software systems from commercial vendors; and
- *Corporate communication networks* that might have an entry point to electricity systems' control networks.

The modern power system also makes extensive use of the global positioning system (GPS), especially for time synchronization. Hence, disruption of GPS by space weather, or through cyber attack, could cause disruption in the bulk power system.

### Operations Error

A number of historical blackouts have been caused by one or more faults, typically when the system is heavily loaded, that could have been managed if not for a sequence of subsequent operator errors. The network structure of the grid allows large-scale disruptions to result from distant, localized electrical faults, and system irregularities can propagate near instantaneously, generally through the work of protection relays acting unexpectedly to unusual system conditions. For example, the infamous 2003 Northeast

blackout was triggered by a simple fault—a tree caused a transmission line short circuit—but within hours it became the largest blackout in U.S. history, owing to two computer/software errors that caused a lack of situational awareness from grid operators. A smaller but similar cascading failure

### BOX 3.1

#### Summary of the Metcalf Substation Attack

In April 2013, the Pacific Gas and Electric-owned Metcalf Transmission Substation outside of San Jose, California, was attacked by one or more gunmen. The attack was well planned and executed, with the attacker(s) severing several fiber-optic cables to disrupt local communications prior to beginning the attack with military-style rifles. In the hour between when communications lines were cut and the first law enforcement officers arrived, 17 transformers had been seriously damaged as oil leaked from bullet holes allowing electric components to overheat. No major outages occurred, as operators were able to re-route power flows from nearby generators, but the attack caused more than \$15 million in damages. Of course, compared with the havoc that would result from a coordinated attack on multiple key substations, the Metcalf event was rather minor.



### BOX 3.2 Summary of the Cyber Attack on the Ukrainian Grid

In a recent, well-publicized cyber attack, approximately 225,000 people were left without power for approximately 6 hours on December 23, 2015, in Ukraine. The attackers gained access to internal networks of three utilities through spear-phishing<sup>a</sup> schemes, malware, and manipulation of long-known Microsoft Office macro vulnerabilities. Rather than try to engineer breaches through the firewall, the attackers patiently harvested the credentials needed to gain access to the supervisory control and data acquisition (SCADA) system and learned how to operate the SCADA software. The attackers executed a well thought out strategy, including the following:

- Creating virtual workstations inside SCADA systems that were trusted to issue system commands;
- Co-opting remote terminal units within SCADA systems to issue “open” commands to specific breakers at substations;
- Severing communications by targeting firmware in serial-to-Ethernet devices, making most unrecoverable;
- Installing and running a modified KillDisk program that deleted information on what was occurring while making recovery reboots nearly impossible;
- Shutting down uninterruptible power supplies at control centers; and
- Executing a large denial-of-service attack on utility call centers that prevented customers from reporting outages and reduced the utilities' understanding of the extent of outages.

These actions prevented operators from accessing the SCADA systems, left control centers without power, and left cyber monitoring and control systems inoperable. Service was restored by shutting off the SCADA system and resorting to manual operation. Although power was restored relatively quickly, control centers were not fully operational for months following the attack (E-ISAC and SANS ICS, 2016).

<sup>a</sup> Spear phishing is a targeted email that appears to be from a known business or individual but is not. It is designed to gain unauthorized access to internal systems by prompting the target to download unwanted software.

occurred in 2011 in the southwestern United States, when a problem at a single substation in Arizona grew into a major outage across Southern California in a few minutes.

There are a vast number of potential types of operations error—in both control rooms and in the field—that can lead to cascading blackouts, which makes planning difficult. Fortunately, because virtually all key components of the power system have protective devices that disconnect before damage can occur, cascading blackouts typically do not cause serious physical damage to system components beyond the initiating failure. Depending on system conditions and the nature of faults, operator error can unfold over periods of minutes to hours, and there may be opportunities to detect errors and take corrective action. With improved training and drilling, better instrumentation, improved situational awareness, and improved control methods, the risks of operator error leading to cascading failure have been, and can continue to be, reduced. At the same time, other external threats such as terrorist attacks and pandemics can place operators under stress and potentially increase the probability of errors. In Figure 3.1, operations errors are denoted by point O.

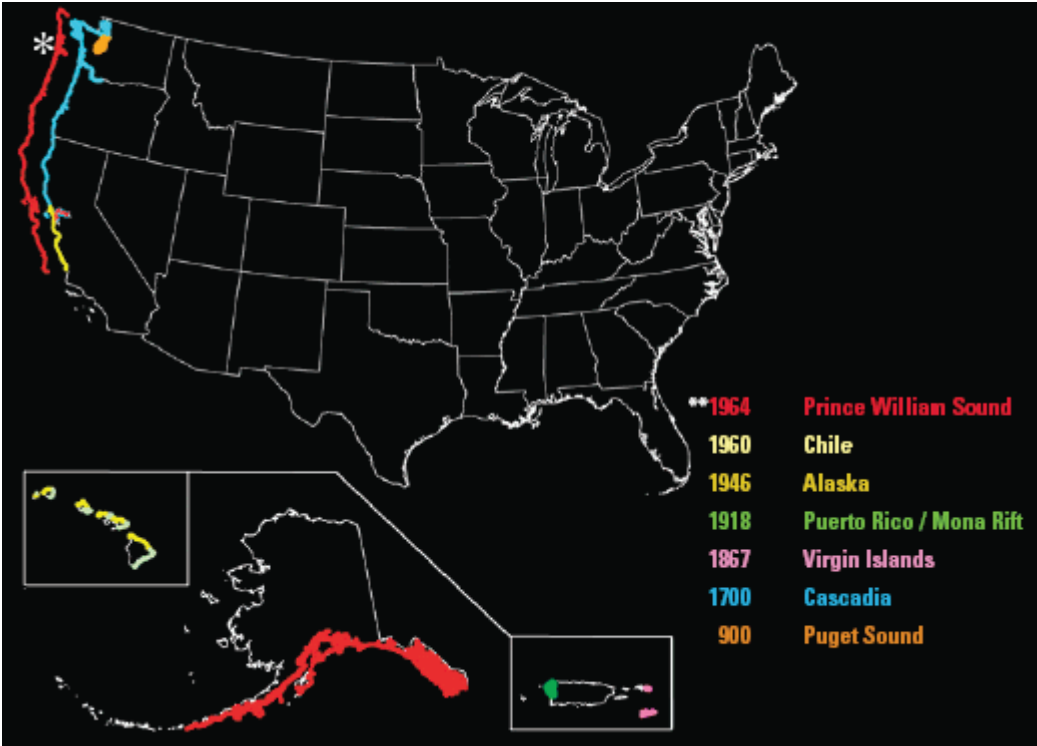
#### Tsunamis

The domain of damage for tsunamis, denoted T in Figure 3.1, is limited to coastal regions. Figure 3.4 shows

locations in the United States that have experienced major tsunami events over the past millennium, which are almost entirely on the Pacific coast. A large international warning system, involving 26 nations, monitors and provides warning across the Pacific basin. As part of that system, the United States hosts the Pacific Tsunami Warning Center near Honolulu, Hawaii, and also operates the Alaska Tsunami Warning Center in Palmer, Alaska. With advance warning, critical facilities can be shut down to reduce damage. Although the best way to reduce the risks to the power system is to place major facilities in locations that are not vulnerable to tsunamis, abandoning and moving existing installations is expensive, and there may be other protective steps that can be taken such as elevating backup generators. This is increasingly a factor in utility planning in Hawaii and along the West Coast.

#### Regional Weather

Weather events can be a major cause of disruption for the power system. Scientific knowledge about both the causes of severe weather events and the ability to detect changes in the risks varies considerably. Some changing risks, such as the likelihood of more frequent and extreme precipitation events and more frequent heat waves, are reasonably well understood in both regards. Others, like the frequency and

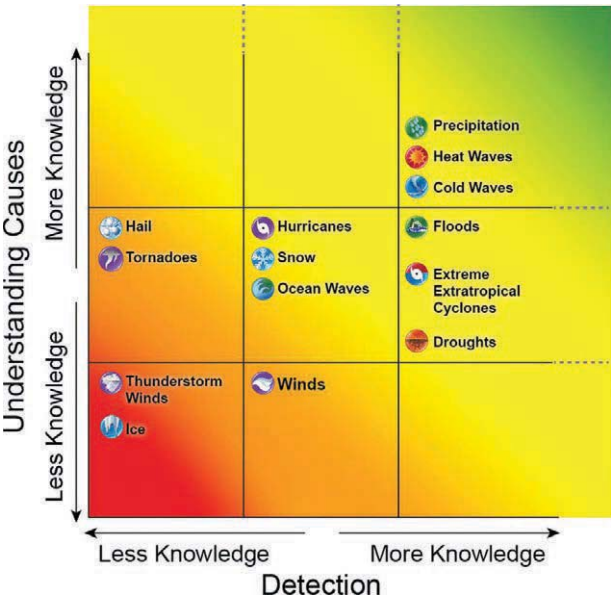


**FIGURE 3.4** U.S. coastal locations that have experienced major tsunamis over the course of the past 1,000 years. SOURCE: USGS (2016a).

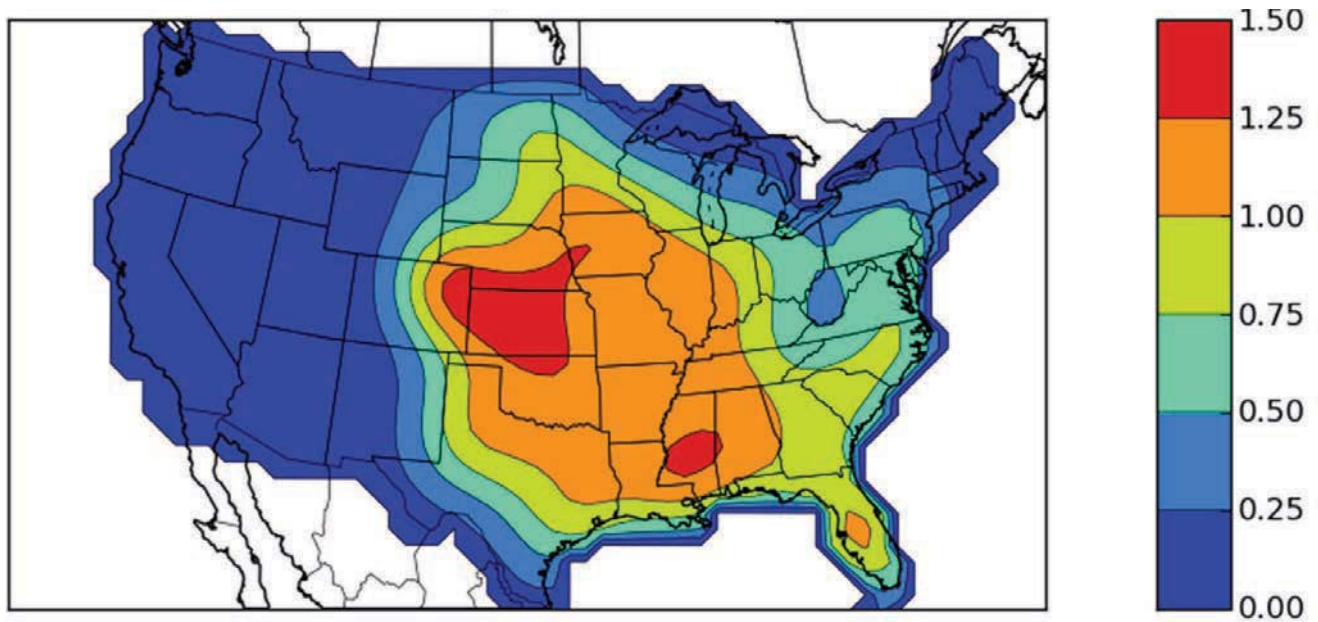
intensity of ice storms (which can devastate power systems), are not understood in either regard. Figure 3.5 displays this considerable variation in the level of scientific understanding of weather and how the frequency and intensity of different weather events may evolve as a consequence of natural variability, climate system oscillations (El Niño–Southern Oscillation, North Atlantic Oscillation, etc.), and secular climate changes (IPCC, 2013; NASEM, 2016).

In Figure 3.1, point R denotes regional weather events such as intense convective storms and tornadoes that are capable of widespread damage, especially to distribution systems. Generally, individual tornadoes impact only a small area, and the specific locations at which damages occur are often difficult to anticipate. However, increasing resolution in weather forecasts does provide system operators with some ability to prepare and be ready to respond quickly once damage has occurred—for example, by pre-positioning repair crews.

Tornadoes have occurred in all parts of the country, but they are rare west of the Rocky Mountains. Similarly, tornadoes do not occur at a uniform rate across the year and are most frequent in April, May, and June (Figure 3.6). Utilities and communities in high-frequency areas are aware of the risk and routinely prepare, building shelters for people and hardening the utility infrastructure.



**FIGURE 3.5** Summary of the state of knowledge of how the frequency and intensity of various weather events may evolve over time. SOURCE: Wuebbles et al. (2014). ©American Meteorological Society. Used with permission.



**FIGURE 3.6** Map of tornado frequency from 1990 to 2009 (days per year within 25 miles of any point). SOURCE: NOAA and NSSL (2009).

The frequency of tornadoes shows a strong temporal and seasonal variation (Figure 3.7). The annual frequency of tornadoes strong enough to cause damage to power lines shows no apparent time trend. On the other hand, Tippet et al. (2016) report that “the largest U.S. effects of tornadoes results from tornado outbreaks . . . we find that the frequency of U.S. outbreaks with the many tornadoes is increasing and that it is increasing faster for more extreme outbreaks.” Tippet et al. (2016) report that, to date, they have been unable to link this increase to climate change. While not ruling out climate change, they speculate that low-frequency climate variability may be a contributing factor, among others. Figure 3.8 shows a track of storms on April 21 and 22, 2006, impacting four states from Mississippi to North Carolina. Often these different events are not connected by local authorities, each of which is responsible for recovery from a fraction of the total impact.

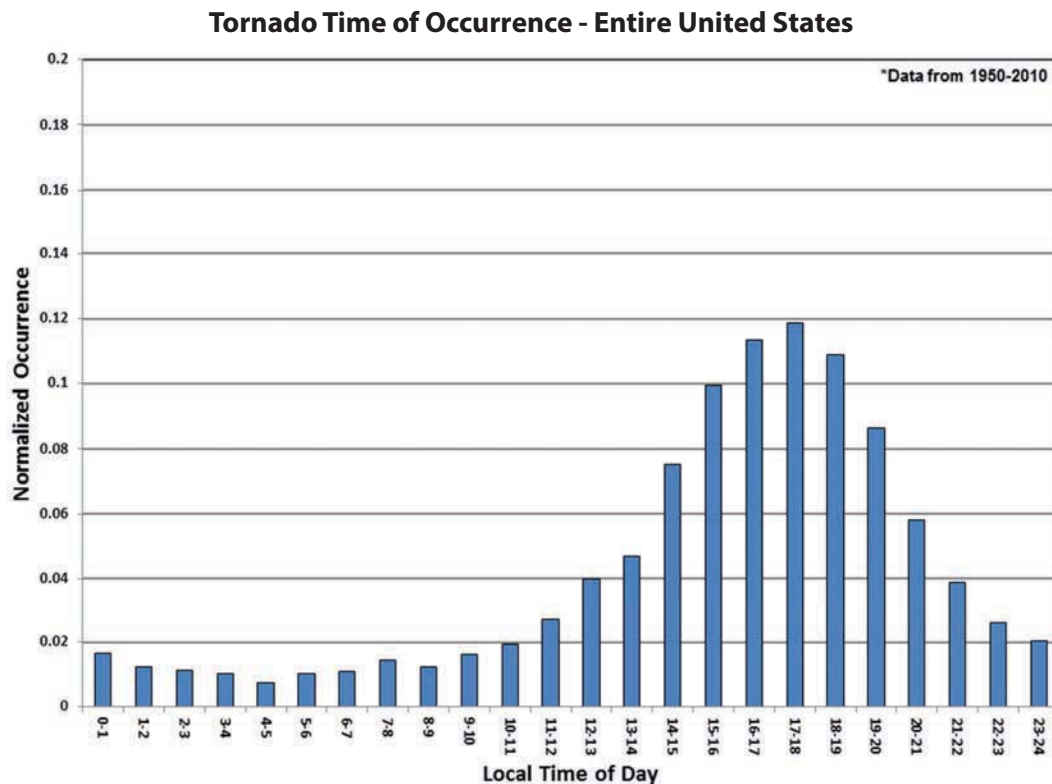
### Ice Storms

Point I in Figure 3.1 denotes ice storms (freezing rain). As is evident from the experience in 1998 in Québec, Ontario, and in upstate New York, ice storms (freezing rain) can result in very widespread damage after which full recovery may take many weeks. Figure 3.9A shows the historical distribution of freezing rain events in the United States over the past 50 years. Figure 3.9B shows the slight upward trend in event frequency over the period 1975 to 2014. Figure 3.9C shows the likely trend in the frequency of future ice storms across the different regions at risk. Ice storms interrupt power through the accumulation of ice on distribution and

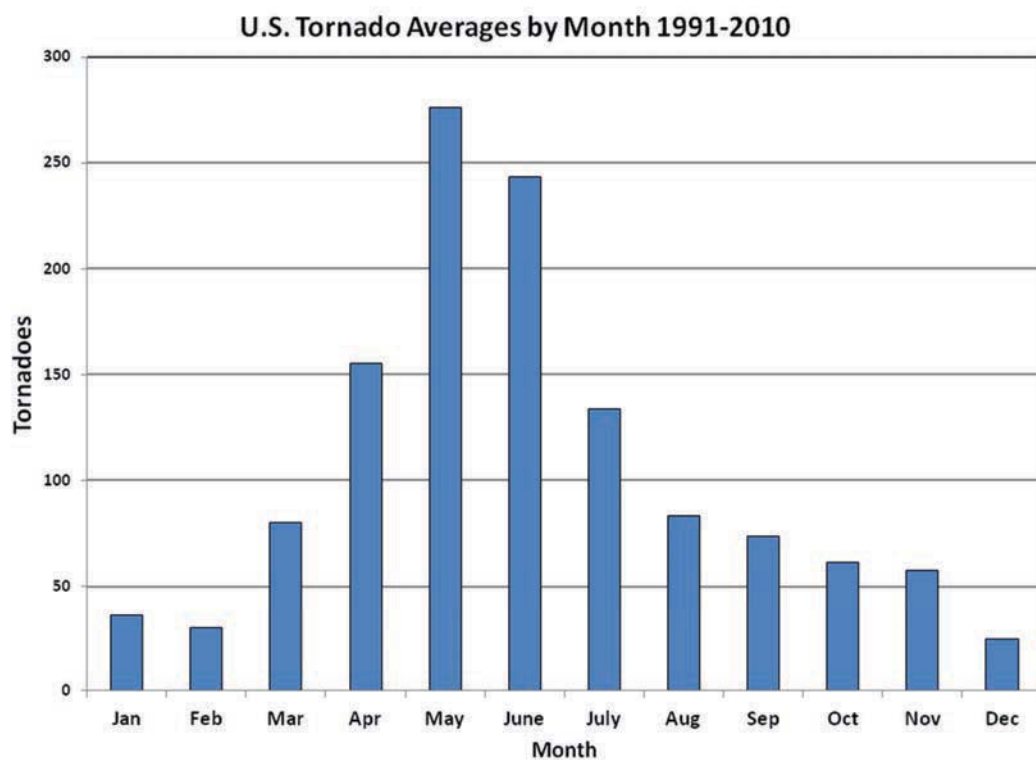
transmission lines, as the added weight brings lines down and causes damage to poles and towers. In addition to increased weight, wind blowing against ice-laden transmission lines can cause low-frequency (1 Hz) high-amplitude (1 m) oscillations (called conductor gallop) that further stress towers and insulators. Ice accumulation on nearby trees can cause branches to fall on lines or bring vegetation close enough to allow arcing current to cause a short. Impacts to distribution systems are common, whereas damage to transmission towers is less common but requires more resources and time to recover from. Many evocative pictures of damaged transmission and distribution infrastructure are available, dating back nearly 100 years. Figure 3.10A illustrates the extent to which ice can accumulate on distribution systems, and Figure 3.10B shows towers that collapsed due to ice accumulation during a massive storm in Québec in 1998. After the first tower failed, others were pulled down.

Winter storms are a leading cause of power outages nationally but do not receive as much national attention as concentrated events like hurricanes. However, they often do not meet Department of Energy (DOE) reporting requirements and might be exempt from the system average interruption duration index and the system average interruption frequency index reliability metric reporting. Because winter storm outages may be underreported, accurate statistics are not available. The majority of outages are relatively localized and handled by utility crews experienced with recovering from them. There are established and emerging techniques to reduce the risk of damage from ice storms and accelerate restoration. Building towers to higher standards is a known strategy, but there is insufficient data on the likelihood of

(A)

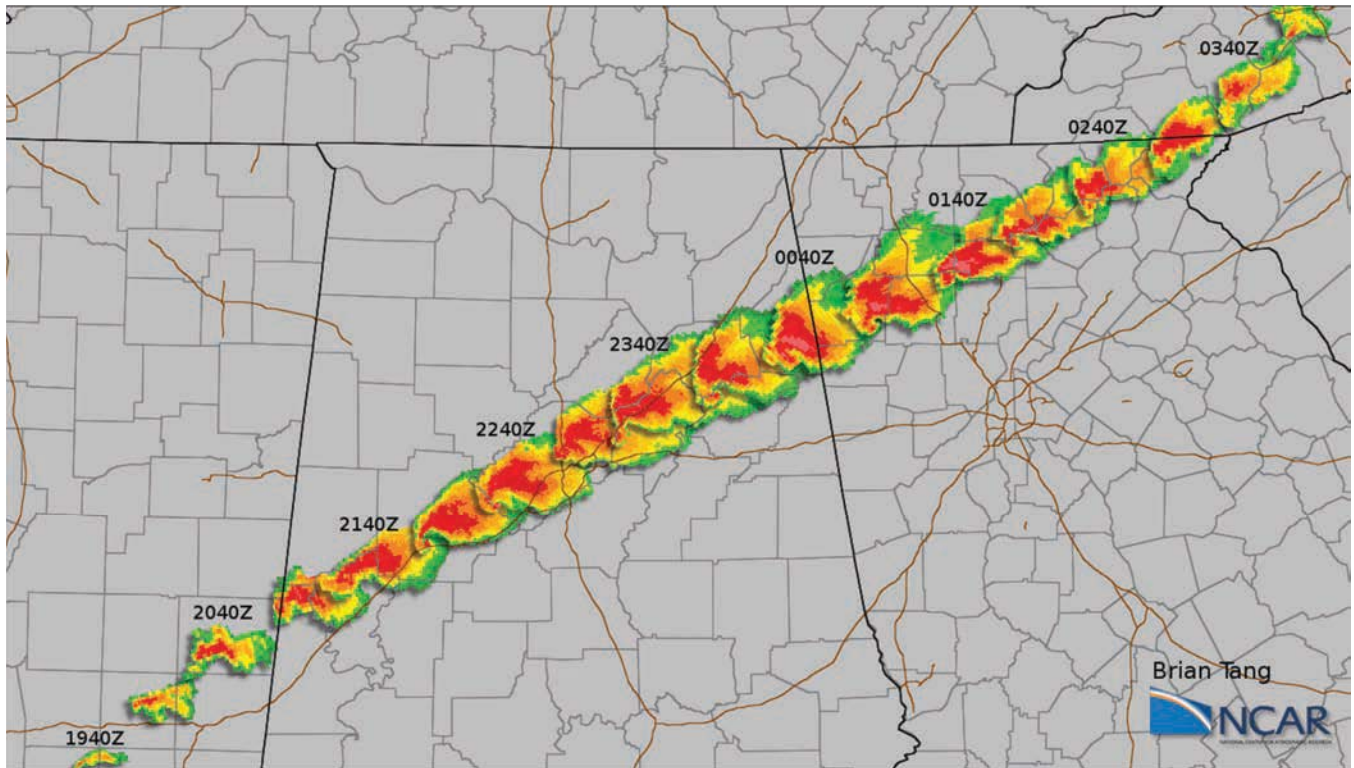


(B)



**FIGURE 3.7** Tornadoes show a strong (A) temporal and (B) seasonal variation.  
SOURCE: NOAA (2016).





**FIGURE 3.8** In 2006, a cluster of tornadoes caused damage across four states in 10 hours from one super cell.  
SOURCE: Tang (2008).

extreme ice events and the associated costs of outages to support greater investment. Techniques being explored for distribution systems include helically staked guying for poles, hydrophilic coating to help electrical infrastructure shed ice, and disconnecting wires that fall to the ground without damaging poles.

### Floods

Floods (Point F in Figure 3.1) can take many forms, from very abrupt flash floods that follow a sudden rainstorm or the breach of a dam, to events whose buildup occurs over extended periods. Floods can damage distribution or transmission towers and their footings or damage equipment installed on the ground. Most utilities have used historical flood data to choose locations for major facilities, such as substations, that are unlikely to be inundated. However, as the climate changes, the frequency of inundation is also changing (e.g., in some places a “100-year event” may have a much more frequent return period).

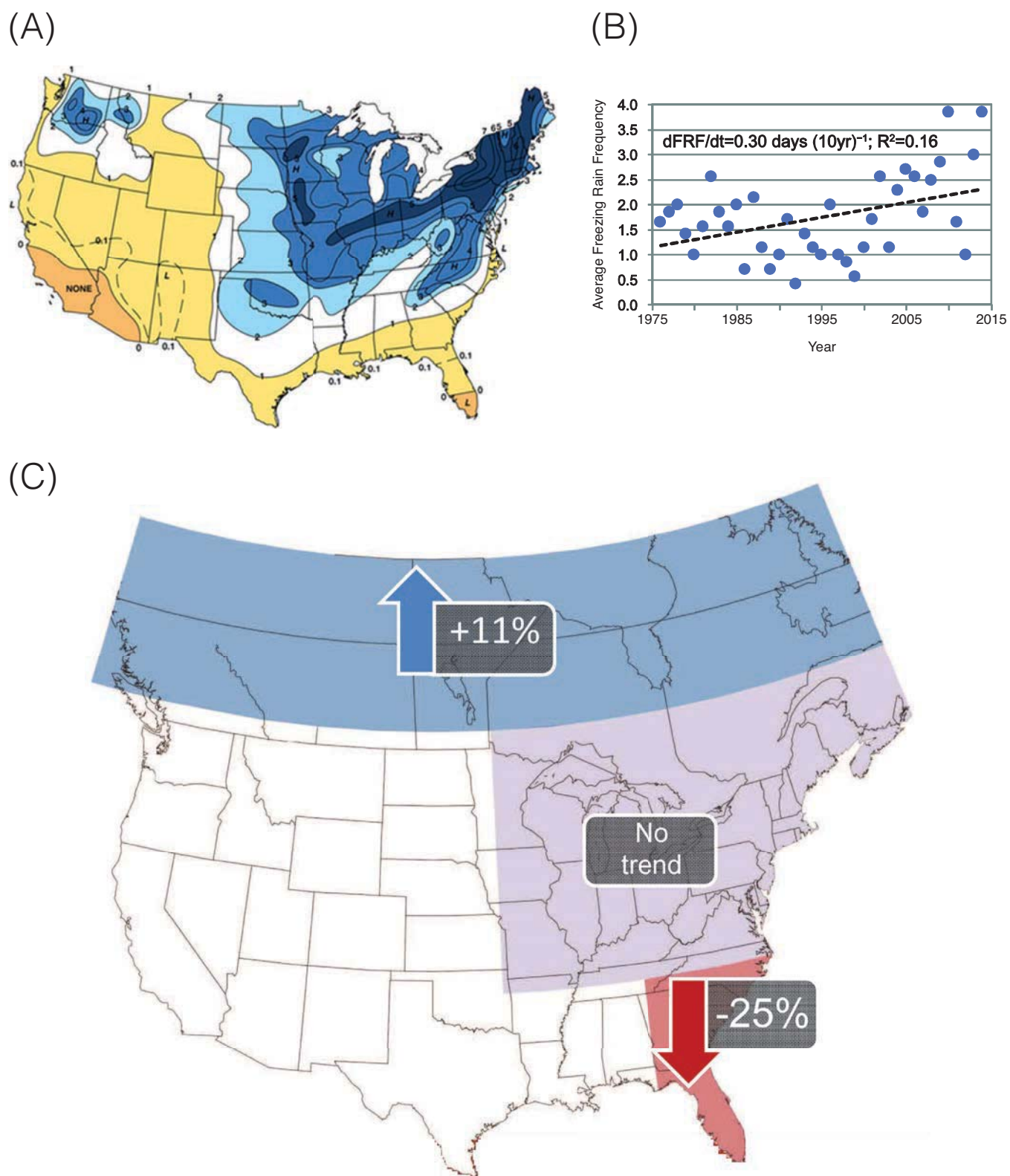
Hurricanes and tropical storms are a principal cause of flooding. Detailed maps of the “100-year flood plan” are available for much of the United States from the Federal Emergency Management Agency (FEMA). As of 2005, about one million miles of stream have been mapped. Figure 3.11 shows an example map for an area impacted by the flood following

Hurricane Agnes. The map reproduced here is compressed (and hence the legends are not readable), but it is included here to convey the type of information that is available.

The Intergovernmental Panel on Climate Change (IPCC) fifth assessment report anticipates that, in light of climate change, North America will experience “an increase in the number of heavy precipitation events” and “increased damages from river and coastal urban floods” (IPCC, 2014). These changes suggest that it is time to explore the development of more informative strategies to communicate the likely extent and frequency of future flooding since the traditional 30-year or 100-year flood metric is problematic when the underlying physical processes are not stationary.

The National Research Council Committee on Floodplain Mapping Technologies examined map accuracy in 2007 in a report titled *Elevation Data for Floodplain Mapping* and recommended much greater use of lidar altimetry (NRC, 2007). There are several challenges to accurate flood mapping, including these two: (1) the changes in the rate of river flows (and height of crest) as land is developed in a watershed, and (2) popular pressure to understate risk to lower flood insurance costs and avert an adverse impact on real estate value. Despite these limitations, the FEMA flood maps, if interpreted conservatively, provide a superb basis for assessing flood risks to electrical assets and planning flood remediation.



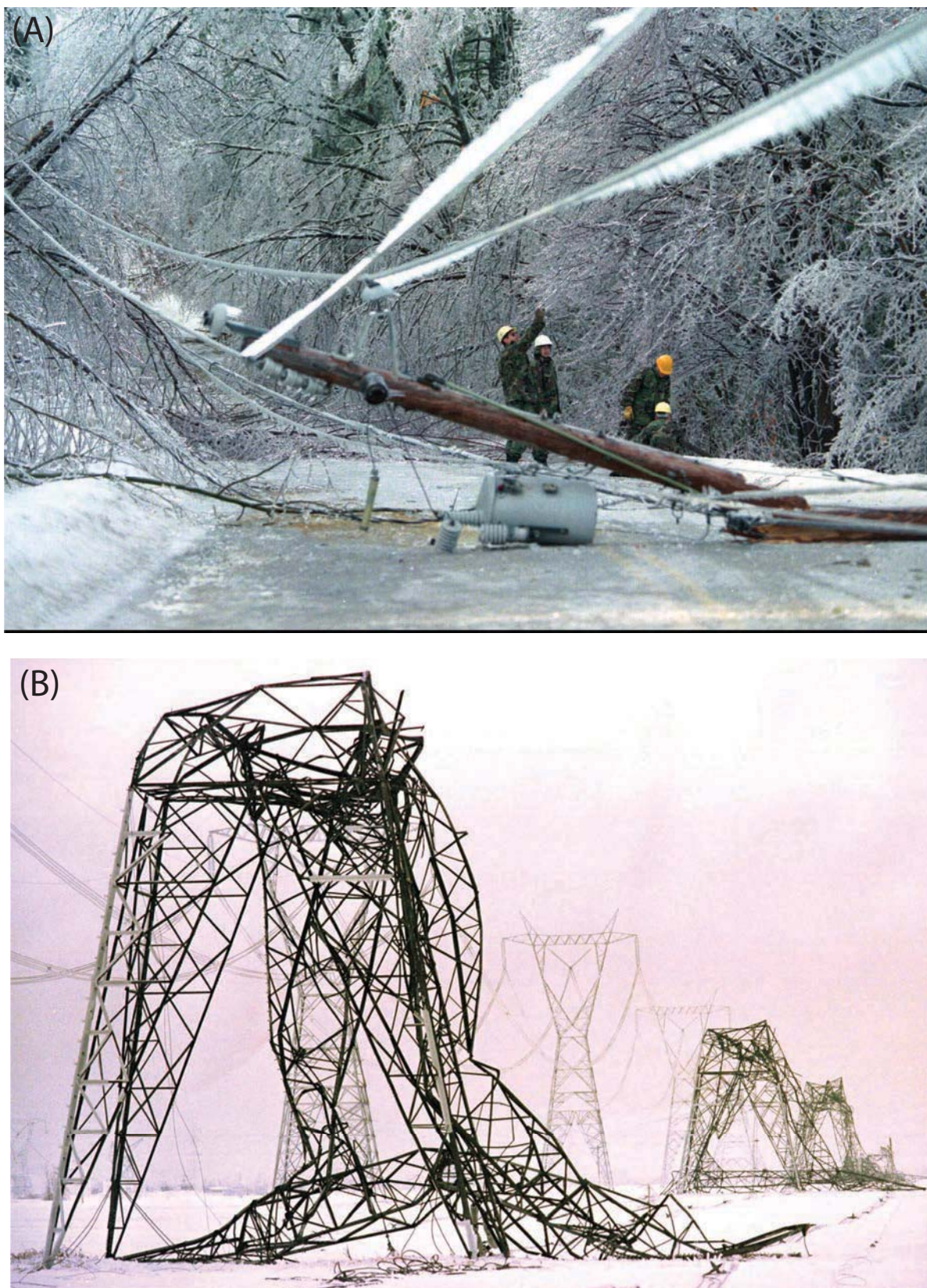


**FIGURE 3.9** (A) Distribution of freezing rain from 1948 to 2000, (B) slight recent trend toward more events, and (C) best estimate of trend by region.

NOTE: FRF, freezing rain frequency.

SOURCES: (A) Changnon and Karl (2003) ©American Meteorological Society. Used with permission. (B) Groisman et al./CC BY (2016). (C) Kunkel (2016).





**FIGURE 3.10** (A) Ice accumulation of several inches on distribution lines caused these poles to collapse, and (B) images from the infamous 1998 ice storm across southeastern Canada and the northeastern United States.  
SOURCE: (A) ©1998 The Associated Press (B) Robert Laberge/AFP/Getty Images.



## THE MANY CAUSES OF GRID FAILURE



**FIGURE 3.11** Example of a Federal Emergency Management Agency flood map for the Susquehanna River near West Pittston, Pennsylvania. The blue shaded areas on the east and west banks of the river are high risk. The dark gray areas beyond the blue area are at moderate risk. The areas outside of the shaded areas are not expected to be impacted by a 100-year flood. SOURCE: FEMA (2016).

In addition to disrupting the bulk power system, flooding can make access difficult for distribution system repair crews, cause damage by flooding manholes, and cause other problems in underground distribution systems and components. This suggests that care should be taken in design and building of underground systems in flood-prone areas.

### Space Weather and Other Electromagnetic Threats

A variety of solar activities (referred to as space weather, point S in Figure 3.1) can impact the earth's environment (NRC, 2008). Large bursts of charged particles ejected by storms on the sun, called coronal mass ejections, can intersect the earth, causing fluctuations in earth's magnetic field that create very low frequency voltage gradients across land, generally at northerly latitudes, and induce quasi-steady-state current that can flow in long transmission lines. These low-frequency currents can cause saturation of transformer magnetic cores and result in damage from overheating. Transformer saturation can also result in reactive power and harmonic generation, which can impact the entire power system. The largest storm of this type in the historical record is the 1859 Carrington Event, which caused telegraph systems

in the United States and Europe to fail. More recently, smaller solar storms have caused blackouts and very limited damage in power systems. In March 1989, approximately 6 million people lost power for up to 9 hours across Québec from a solar storm that damaged a few transformers and other equipment. A smaller hour-long outage occurred in Sweden in October 2003.

A risk summary prepared by Lloyds (2013) argues that “historical auroral records suggest a return period of 50 years for Québec-level storms and 150 years for very extreme storms, such as the Carrington Event.” In a 2011 study, the Department of Defense’s (DOD’s) JASON advisory panel concluded that the federal response to the risk “is poorly organized; no one is in charge, resulting in duplications and omissions between agencies” (MITRE, 2011). In 2015, the North American Electric Reliability Corporation (NERC) published a Notice of Proposed Rulemaking that requires transmission operators to conduct a vulnerability assessment and update it periodically (FERC, 2015). In October 2016, President Obama issued a comprehensive executive order addressing space weather, which gave the Department of Homeland Security overall leadership in geomagnetic disturbance preparedness and the DOE leadership in addressing grid impacts.

In 1989, there was no warning for the impending geomagnetic disturbance, whereas now satellites can provide 30 minutes of advance warning and sun observation up to 2–3 days ahead of impact. This warning could provide utilities an opportunity to protect the grid—for example, implementing operating procedures that are designed to protect critical transformers. The time constants determining impacts on transformers from solar storms (or from the E3 portion of electromagnetic pulse [EMP] events) are slow enough that there is time to protect transformers even as the event is occurring. Developing standard approaches for real time monitoring of transformers that could be susceptible to damage during solar storms (which can be identified through vulnerability assessments required by NERC) would help operators minimize damage. Such real-time monitoring could be combined with automated protection schemes that prevent transformer damage from geomagnetic disturbances. Other engineering solutions exist to make electrical systems more resistant to geomagnetic disturbances, including building better protection into transformers and designing systems to provide more reactive power on demand.

The National Oceanic and Atmospheric Administration (NOAA) and the U.S. Air Force jointly operate the Space Weather Prediction Center that uses solar and satellite observations (including NOAA’s DSCOVR satellite at the L1 point in deep space) to provide forecasts of space weather events. By observing the limb of the rotating sun, the addition of a satellite at L5 could provide valuable additional advance warning (Gibney, 2017). While coronal mass ejections are relatively slow moving, requiring a day or more to reach the earth, there are a number of events that can produce

highly energetic particles that can arrive at the earth in hours, sometimes with little or no warning. These high-energy particles can cause damage to GPS and other satellites, which are used by the power system.

Recent standards for transmission system performance in the event of geomagnetic disturbance (GMD)—for example, NERC standard TPL-007-1—are currently under revision but require that responsible entities maintain detailed system and geomagnetically induced current system models, use these to perform GMD vulnerability assessments every 5 years, and document and communicate this information to other affected entities.

Finally, the committee notes that several of the protective strategies that power companies adopt to reduce vulnerability to solar storms may also provide protection against the lower energy frequencies of an EMP,<sup>1</sup> which is a surge of electromagnetic radiation (Box 3.3) with different components that impact the power system. The early time component of an EMP (E1) is an intense, rapid pulse on the order of tens of kV per meter that decays to nearly zero in less than 1 microsecond; the intermediate time component (E2) has an amplitude of several hundred volts per meter and a duration of one to several hundred microseconds; and the late time component (E3) is a very low amplitude pulse on the order of millivolts per meter with a duration between 1 and 100 seconds. The electric fields associated with EMP can impact power systems directly (E1 and E2) or induce currents in transmission lines similar to the low frequency currents associated with GMD events (E3). Small, suitcase-size EMP devices<sup>2</sup> can also cause electromagnetic disturbances that can impact the power systems' (especially substation) equipment, but the impacts will likely be very localized. A nuclear weapon or a dedicated non-nuclear EMP device detonated at a high altitude could cause widespread damage to the electricity grid; nonetheless, understanding of this risk is largely theoretical. The Electric Power Research Institute (EPRI) collaborated with DOE recently to develop a Joint Electromagnetic Pulse Strategy that outlines broad objectives and research needs but stops short of presenting a plan for EMP hardening (DOE and EPRI, 2016).

While most critical satellites have been “hardened,” a large enough space weather event could cause damage to earth-orbiting satellites including those used for communication and the GPS. Modern utilities use the GPS to provide time synchronization across their spatially distributed systems. Disruption of these precise timing signals can result

<sup>1</sup> A continental-scale electromagnetic pulse caused by the detonation at high altitude of a specially designed nuclear weapon consists of several electromagnetic waveforms, the first of which has an extremely rapid rise time.

<sup>2</sup> “Suitcase-size EMP devices” are more accurately referred to as radio frequency weapons, essentially a class of non-nuclear weapons that have a local impact similar to that of an EMP E1 pulse. While the DOD is very experienced in this area, less attention has been directed to protecting civilian infrastructure. The concern is that one of these devices might target a control center, disrupting some or all of its computers and communications.

### BOX 3.3 Electromagnetic Pulse

An electromagnetic pulse (EMP) is a short duration surge of electromagnetic radiation that can be human-made or natural in origin and have local or widespread impacts. While local impacts can be caused by lightning strikes or by radio-frequency weapons, wider EMP impacts could be caused by the high-altitude detonation of an appropriately designed nuclear weapon. Such a wide-area EMP induced by a high-altitude nuclear weapon is an issue most appropriately addressed by the DOD.

The DOE and EPRI (2016) created the Joint Electromagnetic Pulse Resilience Strategy to help reduce the grid's vulnerability to EMP and improve the energy sector's response and recovery. The initial plan is more of a research strategy than an actual plan for EMP hardening and will take several years to realize. The plan sets five objectives:

1. Improve and share understanding of EMP threat, effects, and impacts;
2. Identify priority infrastructure;
3. Test and promote mitigation and protection approaches;
4. Enhance response and recovery capabilities to an EMP attack; and
5. Share best practices across government and industry, nationally and internationally.

in operational problems. While the GPS is well protected, it is also possible that sophisticated earth-bound hackers could disrupt GPS software and control systems. There are technologies that can minimize this risk, but to date their adoption has been limited (Achanta et al., 2015).

### Hurricanes or Tropical Cyclones

As we have learned repeatedly, tropical cyclones can create enormous havoc in power systems. Modern forecasting methods typically provide several days of advance warning, with increasingly more precise and accurate predictions about intensity and the location of landfall as a storm comes closer. Over their lifetime, tropical storms have three basic impacts on power systems: (1) initial impact of wind and rain, (2) storm surge in coastal areas and near major inland waters (e.g., Lake Pontchartrain during Katrina), and (3) flooding due to precipitation. Hurricane risk is concentrated on the Atlantic and Gulf coasts of the United States and in the state of Hawaii (Figure 3.12A).

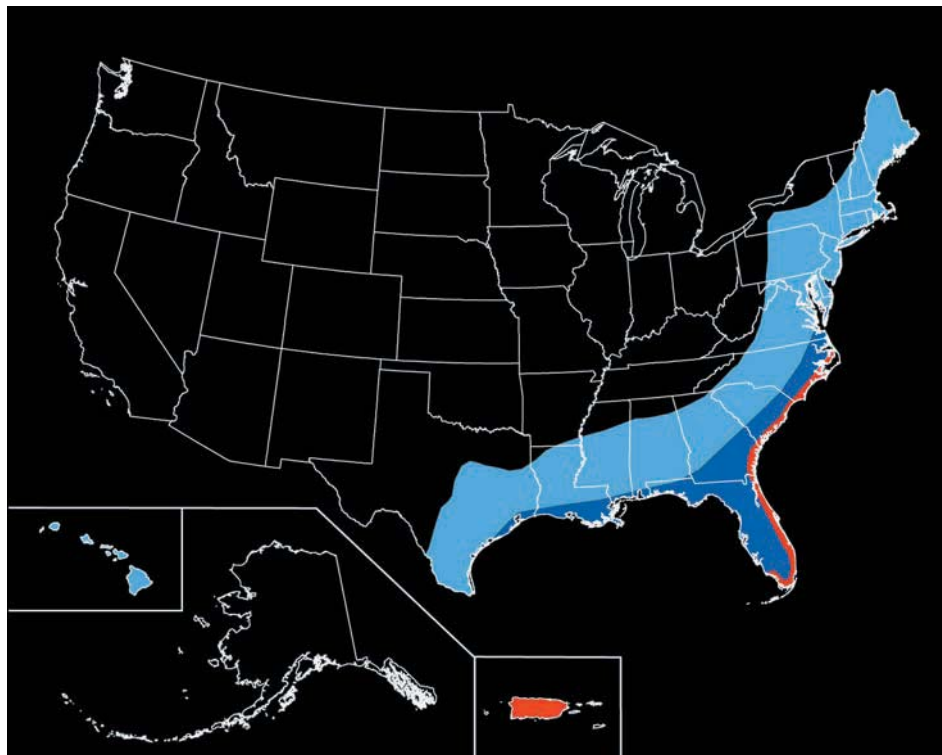
A 2016 report of the National Academies of Sciences, Engineering, and Medicine concludes that a “broad consensus

## THE MANY CAUSES OF GRID FAILURE

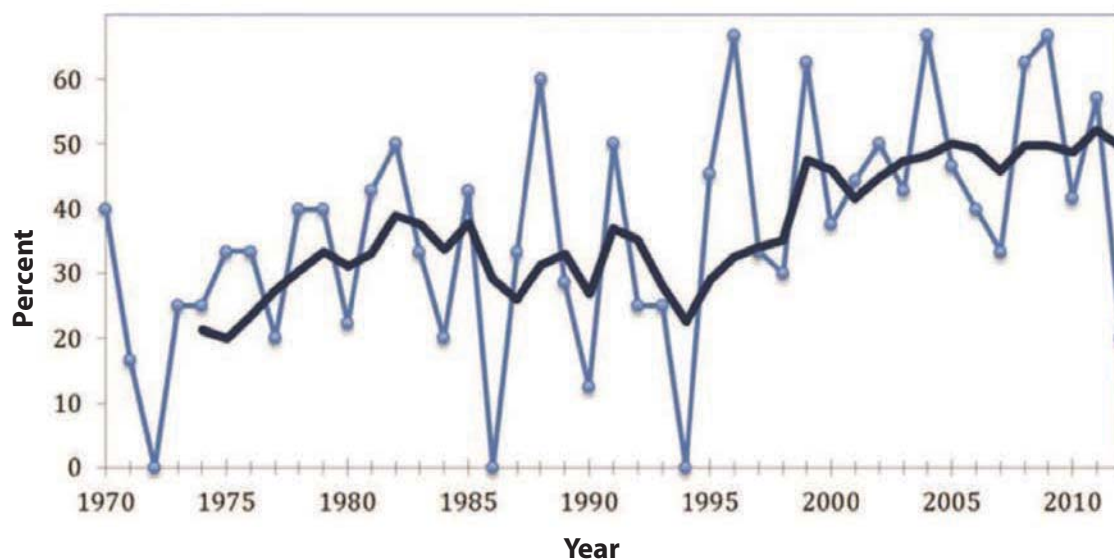
has emerged as to the expected future trends in their levels of certainty . . . tropical cyclones are projected to become more intense as the climate warms. There is considerable confidence in this conclusion . . . the global frequency of tropical

cyclone formation is projected to decrease . . . but there is less confidence in this conclusion than in the expectation of increasing intensity,” as indicated with historical data in Figure 3.12B (NASEM, 2016).

(A)



(B)



**FIGURE 3.12** (A) The region of hurricane risk is greatest on the Atlantic and Gulf coasts of the United States and (B) recent years have seen a trend of Atlantic hurricanes becoming more intense. This is probably the result of both warmer sea-surface temperatures and natural climate variations. The lighter color line is the percentage of hurricanes that reach category 3 or greater each year, and the dark is the 5-year running average.

SOURCE: (A) The National Atlas and USGS (2005) and (B) UCS (2016) at [www.ucsusa.org](http://www.ucsusa.org).



Along with winter storms, hurricanes and tropical storms<sup>3</sup> (Point H in Figure 3.1) are some of the largest sources of disruption of power systems. As illustrated by Superstorm Sandy and Hurricane Katrina, the resulting destruction can be widespread. Sandy was an immense and meteorologically complex storm that caused outages in 17 states and the District of Columbia, with the impacts beginning over a relatively short period of time. In contrast, Hurricane Katrina was a very different storm. While its impact on New Orleans (due largely to dike failures) and coastal Mississippi was the focus of press coverage, the total impact on electricity infrastructure was much broader because the storm had more rainfall, had higher sustained wind speed over larger areas, and traveled up the Mississippi River valley causing outages as far inland as Tennessee. Both Katrina and Sandy were devastating, but while Sandy was essentially a concentrated event, Katrina caused damage to power systems across a much larger region. While advanced models allow scientists to project the course and development of hurricanes with greater precision than ever before, weather events still have the capacity to surprise. In planning and preparation, it is important to remember that the evolution of a hurricane can involve substantial uncertainty.

### Volcanic Activity

In much of the country volcanic activity (V in Figure 3.1) is not a concern, but in the Pacific Northwest, and parts of Alaska and Hawaii, it presents a low probability but high consequence risk from eruption, ash fall, lava flow, and lahars. The U.S. Geological Survey maintains an active warning program (USGS, 2016b). Clearly the best strategy to avoid problems is to locate critical facilities away from vulnerable locations. However, as Figure 3.13 illustrates, in the case of Mount Rainier, the impacted region can be quite large. Additional damage can be caused by fine particulate dust and falling ash, which can cause insulator flashovers and potentially disable transformers. The geographic extent of falling ash may greatly exceed the immediate hazard area.

### Wildfire

Climate scientists have long predicted more frequent and more intense wildfires as a result of ongoing climate change (NCAR, 1988). While fire typically does not cause widespread damage to power systems, it can have major impacts on specific substations and transmission systems, and operators may have to re-route power flows to avoid affected areas. Vulnerability can often be limited with vegetation control, although very large fires can often jump even the most aggressive protective margins. Restoration of fire-damaged

facilities can require days or weeks. Fire is denoted as point W in Figure 3.1.

### Drought

Finally, in the extreme upper right corner of Figure 3.1 is point D, for drought. Droughts have multiple implications for power systems, ranging from reduced hydroelectricity generation, limited availability of cooling water for power stations, or increased demand for power needed for pumping and treatment. The IPCC report on extreme events concluded that “there is *medium confidence* that droughts will intensify in the 21st century in some seasons and areas, due to reduced precipitation and/or increased evapotranspiration. This applies to regions including . . . central North America” (Seneviratne et al., 2012).

While the power system can become very stressed during extreme heat (heat waves), ordinarily it manages to deal with such events. Of course, when the power system is highly stressed, the probability of hardware failures or operator error resulting in significant outages increases. The IPCC Fifth Assessment Report (2014, p. 10) concluded, “It is *virtually certain* that there will be more frequent hot and fewer cold temperature extremes over most land areas on daily and seasonal time scales, as global mean surface temperature increases. It is *very likely* that heat waves will occur with a higher frequency and longer duration.” The 2014 U.S. National Climate Assessment drew similar conclusions (USGCRP, 2014).

### Findings and Recommendations

The hazards reviewed in this section fall broadly into two categories: (1) those in which human action is the primary contributing factor, and (2) those that involve natural causes. The committee divides its findings and recommendations in this same way. With respect to hazards resulting from human actions, the committee finds the following:

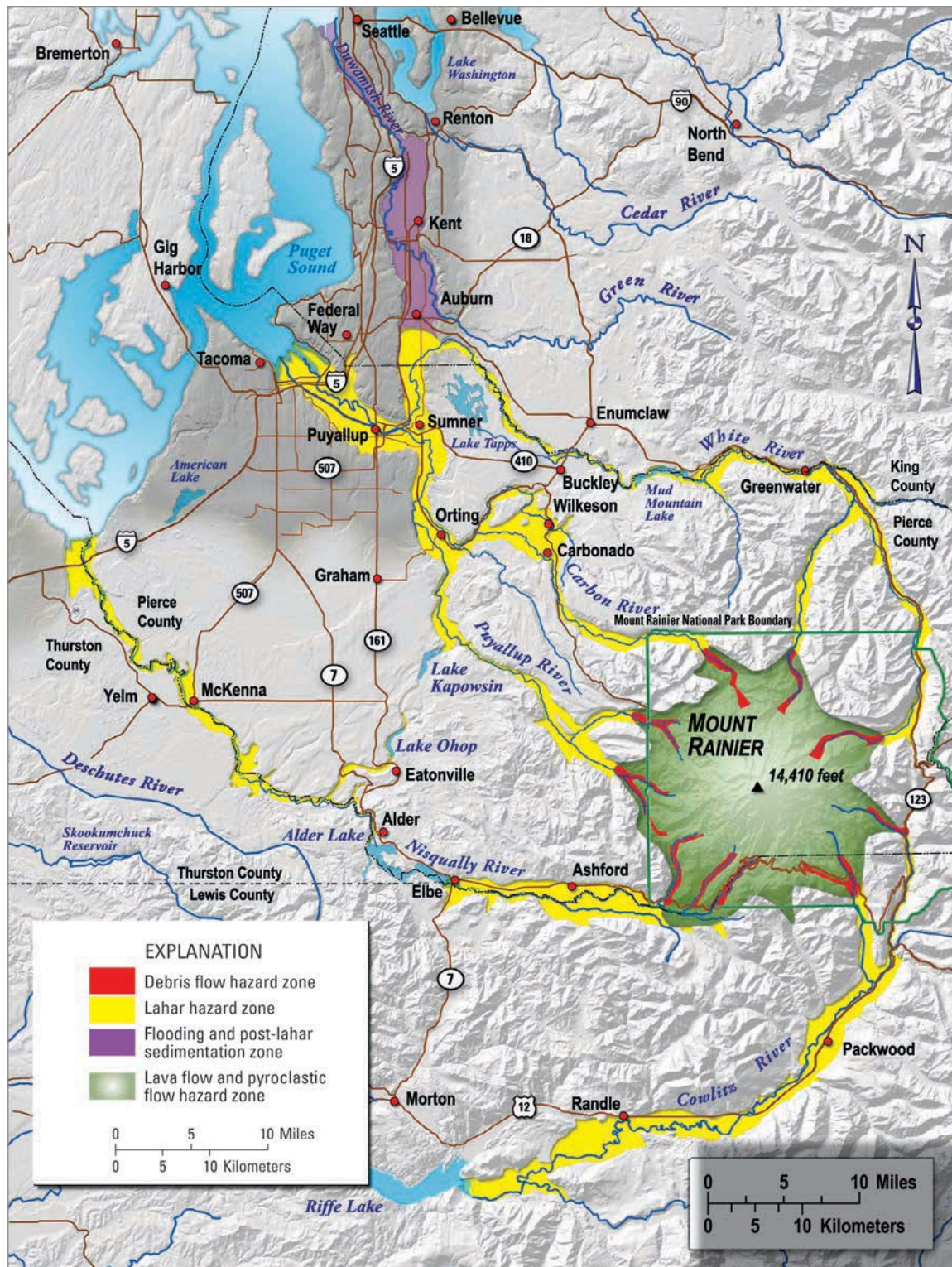
**Finding:** While to date there have been only minor attacks on the power system in the United States, large-scale physical destruction of key parts of the power system by terrorists is a real danger. Some physical attacks could cause disruption in system operations that last for weeks or months.

**Finding:** The United States has been fortunate that none of the cyber attacks that are being mounted against the power system have caused significant service disruption. However, the risks posed by cyber attacks are very real and could cause major disruptions in system operations.

**Finding:** While it is tempting to think of physical and cyber attacks as separate and discrete hazards, they could occur together and could also occur repeatedly. Furthermore, because the power system is essential to the operation of

<sup>3</sup> In this discussion, the committee includes post-tropical cyclones like Superstorm Sandy where most of the damage was done after the winds had dropped below hurricane force and the storm had lost its hurricane structure.

## THE MANY CAUSES OF GRID FAILURE



**FIGURE 3.13** Volcanic hazard map for the region around Mount Rainier. A “lahar” is a mud and debris flow that can bury everything in its path such as the communities marked as “hazard zones.”

SOURCE: USGS (2008).



many important infrastructures, physical and/or cyber attacks on that system can impact delivery of other critical services. An attack on the power system undertaken in conjunction with other terrorist action could be especially harmful.

**Recommendation 3.1:** To better protect the grid from physical and cyber attacks, the intelligence communities, the Department of Homeland Security, the Department of Energy, and operating utilities should sustain and enhance their monitoring and information-sharing activities and continue to assure that adequate communication channels are maintained among all responsible parties. Additional steps, such as the creation of teams to test weaknesses in existing systems, should be taken to avoid the risks of complacency and to drive a culture of continual improvement.

With respect to hazards resulting from natural causes, the committee finds the following:

**Finding:** Good data on the causes, probabilities, and spatial and temporal distribution of natural hazards that can disrupt power systems are essential to assuring the resilient operation of those systems. Government and other responsible parties should support and strengthen the activities of organizations that collect these data.

**Finding:** The probability, intensity, and spatial distribution of many of the hazards that can disrupt the power system are changing. These changes are due in part to the consequences of ongoing climate change. Traditional measures, based on an assumption of statistical stationarity (e.g., 100-year flood), may need to be revised to produce measures that reflect the changing nature of some hazards.

**Finding:** Some organizations that are responsible for monitoring and preparing for natural hazards, such as floods and tornadoes, have a local focus that can overlook spatial correlation and broader system risks. Nonetheless, local assessments such as the “Threat and Hazard Identification and Risk Assessment,”<sup>4</sup> encouraged by the Federal Emergency Management Agency, can provide valuable resources for utilities to build upon.

**Recommendation 3.2:** On a periodic basis (e.g., every 5 years), the Department of Homeland Security and the Department of Energy, as the energy sector lead, should work with state and local authorities and electricity system operators to undertake an “all-hazards” assessment of the natural hazards faced by power systems. Local utilities should customize those assessments to their local conditions and build on existing local assessments to include detailed electricity

system information, keeping in mind that the past may not be an accurate predictor of the future.

## THE LIFE CYCLE OF A POWER OUTAGE

Although the type and extent of damage varies among the different threats previously described, a notional time-series model of a power outage is shown in Figure 3.14, which provides elaboration of some of the key steps in the four-stage process of resilience displayed in Figure 1.2A. The committee also uses these steps in Chapter 6 to illustrate strategies to achieve resilience in the face of a specific cause of disruption.

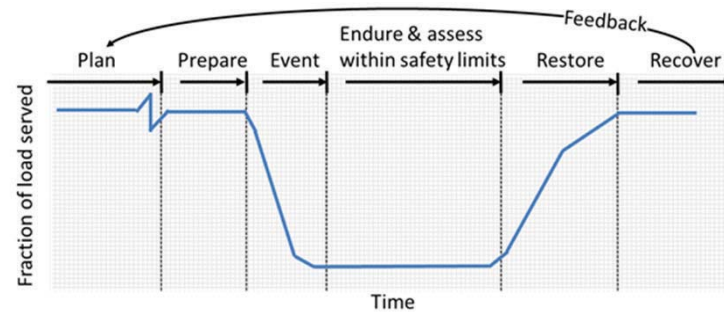
The blue line in Figure 3.14 illustrates the percentage of load that may be served over time, from the initial full level until the start of the event, at which point load begins to drop off. Load persists at a reduced level for some period until restoration begins. Power is then restored, although sometimes not to the full pre-event level, as electricity-consuming entities may have been damaged or destroyed. If the event caused significant physical damage, load may continue to build slowly during a multi-year recovery period as electricity systems are restored, homes are reoccupied, and businesses reopen.

The relative length of each stage and the activities undertaken by utilities and other organizations involved in the response are different depending upon the type of disruption. Likewise, the activities undertaken by utilities during each of these stages also varies significantly based on the resources available and the technological characteristics of the impacted system. As briefly introduced below and as outlined in the following chapters, there are many strategies that can help utilities perform better through the entire outage life cycle.

## Plan

The majority of time is spent in the planning stage, which occurs continuously and well before any specific hazard is identified. While there is variation among organizations, utilities—from large vertically integrated firms to small distribution cooperatives—generally know what the major hazards are in their service territories, may have first-hand experience with such hazards, and may even be required by regulators to prepare and submit plans regularly for addressing these risks. For example, utilities in the Southeast prepare for hurricanes, whereas those in the far northeast focus more on ice storms. Utilities also generally know which parts of their physical systems are most vulnerable. This knowledge is acquired through experience and with diverse resources, such as data sets from NOAA and the National Weather Service. Nonetheless, the local impacts of most hazards, even those with a long history, are unknown during planning stages. Following Superstorm Sandy, the New Jersey utility Public Service Enterprise Group believed that the impact would have been much greater (perhaps double) if the storm track had been only 10 miles different, as more

<sup>4</sup> See, for example, [https://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201\\_htirag\\_2nd\\_edition.pdf](https://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf).



**FIGURE 3.14** Notional time series of a major power outage divided into six stages. The length of each stage and the activities performed by utilities and others involved in the response vary for different disruptions.

critical substations could have been affected by flooding in drainage basins. Utilities have less experience handling certain risks—notably those related to cyber attack—which makes assessing and planning more difficult.

Activities during the planning phase are both preventative and preparatory. At the distribution level, these include hardening system components and installing more advanced technologies such as automatically reconfigurable circuits. The level of investment by different utilities is closely tied to state regulatory or board oversight decisions; thus, there is wide variability across different states, and planning decisions are not solely determined by utilities. For investor-owned utilities, state regulatory commissions strive to keep costs low for ratepayers by approving investments that have net benefits for customers and not allowing a utility to “gold plate” its system. On the transmission level, utilities maintain, harden, and expand the physical and cyber infrastructure (both hardware and software) with investments and reliability standards overseen by NERC and FERC. As the complexity and scale of the grid as a cyber-physical system continues to grow, there are opportunities to plan and design the system to reduce the criticality of individual components and to fail gracefully as opposed to catastrophically. Equally important, utilities routinely plan for restoration—for example, by developing mutual assistance agreements, investing in spare parts sharing programs, and conducting restoration drills and exercises. Utilities must also engage and maintain strong relationships with local emergency management agencies to integrate their own planning into local and national efforts, as discussed in greater detail in Chapters 5 and 6. Additionally, there is a critical need to engage electricity end users during planning to define the locations and characteristics of critical loads in a service territory and ensure appropriate use of backup generation.

### Prepare

The preparation phase begins when a specific threat is identified—for example, when a hurricane forms with a projected track that will impact a specific utility. Some hazards have no advance warning, while others can be identified and

monitored with sufficient time for utilities and other responders to move beyond general planning and develop specific actions. For example, utilities preparing for impending hazard may check the health of critical components (including the health of cyber systems), check stocks of spare equipment, activate mutual assistance agreements, and bring local crews to a state of readiness, potentially pre-staging supplies and repair crews at specific locations. Operators assess the level of generation available, likely bringing additional reserve generation online, evaluate the adequacy and vulnerability of different fuel stocks and supply chains, and verify the state of charge of utility-scale storage assets if available. During preparation, utilities can begin coordinating with relevant disaster response organizations and encourage the public to purchase fuel and test backup generators. Utilities that have built and maintained strong relationships with local emergency management organizations know whom to engage, whereas organizations that have not built these relationships may waste valuable time and resources trying to connect with local efforts. There are growing opportunities to engage distributed energy resource (DER) owners so that system operators know the state of these resources, although current interconnection standards and contractual arrangements need to be revised to promote utility visibility and controllability of DERs.

### Event

The duration of disruptive events varies significantly, as do the capabilities and resources of different utilities. The duration of the actual disruptive event is always much shorter than the period from planning through final recovery. It can last many hours for hurricanes to minutes or even seconds for tornadoes and earthquakes. Floods can last many days or a small number of weeks. The longest duration, however, is for cyber events. The outage may only last a short time, but the period from cyber breach to detection and remediation may last many months. In the recent hack in Ukraine, the breach occurred 9 months before power was interrupted. The hackers used this time to learn how to control the breached systems.

Except in the case of a cyber attack, when the event may be ongoing for an extended period but undetected, the principal activity during the event is to monitor the damage and failures as they emerge and to develop as clear an understanding of system state as possible. Distribution systems with large amounts of advanced meter infrastructure and automated reconfiguration may lessen the number of customers experiencing outages. Some utilities may not be aware of outages until they are reported by telephone. Some events may be so destructive to physical and cyber systems that automation technologies have no benefit and could even be detrimental in the case of a cyber attack (e.g., if microprocessor-based relays with software installed by the manufacturer are hacked, the utility may have to replace the relay entirely or send it back to the manufacturer). There is a great deal of activity at the level of generation and transmission systems. System operators can balance generation and load through generation dispatch, load control (e.g., rolling blackouts), controllable DERs, or intentional islanding. It may be possible to continue with some preparatory activities, but, with limited time, telemetry, and communications, major changes may not be possible.

### Endure and Assess Within Safety Limits

For some events, conditions may prevent dispatch of crews (either boots on the ground or manned or unmanned aerial vehicles) because of safety concerns. This period may be zero (i.e., restoration can begin immediately), or it may stretch for a lengthy time if access to damaged facilities is blocked as by floodwater or landslides (utility crews can usually deal with downed trees). If cyber monitoring and control systems are intact, utilities can continue to assess the state of the system. During this phase, utilities communicate to understand the extent of damage, begin to prioritize repairs based on available information, and may even schedule the dispatch of restoration crews. As explained in Chapter 5 of this report, there are many strategies to reduce the adverse social and economic impacts of power outages, including using DERs, backup generators, and microgrids to provide local power to critical facilities.

### Restore

Restoration is the most tangible and publicly visible phase of the event life cycle. As soon as conditions permit safe dispatch of crews, utilities develop a high-resolution understanding of damages with manned and unmanned aerial vehicles as well as crews on the ground. Based on this understanding, priorities for restoration are established and repairs initiated, often through the shared resources previously arranged in mutual assistance agreements. If a critical transformer without a replacement is damaged, the system may have to be operated in a reduced state until a suitable replacement can be provided. System operators manage switching to

support physical restoration. Central operations also provide information to customers and support field crews by providing the necessary materials, replacement components, repair equipment, and qualified workers, as well as transportation and provisioning. This may require coordinating with state or federal officials to waive regulations or even using military resources in extreme cases. If there are regions of the interconnection with power, restoration may proceed from the “edge”; alternatively, utilities may initiate black-start<sup>5</sup> procedures. As installations of DERs continue to increase, there are growing opportunities to use these resources in restoration and black start; however, significant research is needed to demonstrate this capability.

### Recover

After the electrical grid has been repaired and service has been restored from a large-area, long-duration outage, utilities and regulators typically evaluate the event to identify root causes and opportunities to improve performance. These investigations directly inform planning and investment decisions made by utilities and overseen by regulators. As discussed in later chapters, there is often scrutiny of utility and infrastructure performance following a major outage, and there may be public and political support for grid investments that impact regulatory proceedings. In many cases (excluding cyber attacks and cascading failures) the commercial, residential, and public infrastructure are also damaged, may be long in returning, or may be lost permanently. In this case, the immediate restoration may be concluded, but the load served may be slightly or substantially less than prior to the event. Presuming the economy recovers and the impacted region is restored, the utility may be engaged in new construction for a number of years. At a minimum, this will entail a sustained period of increased capital spending and staffing for construction.

### REFERENCES

- Achanta, A., S.T. Watt, and E. Sagen. 2015. Mitigating GPS Vulnerabilities. Presented at the *Power and Energy Automation Conference*, Spokane, Wash. <https://selinc.com/api/download/104197/>. Accessed April 15, 2017.
- Argonne National Laboratory, Brookhaven National Laboratory, Los Alamos National Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, and Sandia National Laboratories. 2016. *Resilience of the U.S. Electricity System: A Multi-Hazard Perspective*. <https://energy.gov/sites/prod/files/2017/01/f34/Resilience%20of%20the%20U.S.%20Electricity%20System%20A%20Multi-Hazard%20Perspective.pdf>.
- Changnon, S.A., and T.R. Karl. 2003. Temporal and spatial variations of freezing rain in the contiguous United States: 1948–2000. *Journal of Applied Meteorology* 42(9): 1302–1315.

<sup>5</sup> Most generators require power from the grid to energize their windings, which will not be available in the event of a major outage. “Black start” refers to the process of providing the necessary power to restore a generation plant when grid power is unavailable.



## THE MANY CAUSES OF GRID FAILURE

- DOE (Department of Energy). 2015. "Modernizing the Electric Grid." *Quadrennial Energy Review First Installment: Transforming U.S. Energy Infrastructures in a Time of Rapid Change*. <https://energy.gov/sites/prod/files/2015/08/f25/QUER%20Chapter%20III%20Electricity%20April%202015.pdf>.
- DOE and EPRI (Electric Power Research Institute). 2016. *Joint Electromagnetic Pulse Resilience Strategy*. [https://www.energy.gov/sites/prod/files/2016/07/f33/DOE\\_EMPStrategy\\_July2016\\_0.pdf](https://www.energy.gov/sites/prod/files/2016/07/f33/DOE_EMPStrategy_July2016_0.pdf).
- E-ISAC (Electricity Information Sharing and Analysis Center) and SANS ICS (Industrial Control Systems). 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. [https://ics.sans.org/media/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_5.pdf](https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf).
- FEMA (Federal Emergency Management Agency). 2016. "FEMA Flood Map Service Center." <http://msc.fema.gov/portal>. Accessed February 28, 2017.
- FERC (Federal Energy Regulatory Commission). 2015. "FERC Proposes New Reliability Standard on Geomagnetic Disturbances." <https://www.ferc.gov/media/news-releases/2015/2015-2/05-14-15-E-1.asp#.WJS-5jm8rLGh>. Accessed March 2017.
- Gibney, E. 2017. Europe lines up for solar storm view. *Nature* 541: 271.
- Groisman, P.Y., O.N. Bulygina, Y. Xungang, R.S. Vose, S.K. Gulev, I. Hanssen-Bauer, and E. Førland. 2016. Recent changes in the frequency of freezing precipitation in North America and Northern Eurasia. *Environmental Research Letters* 11(4): 045007.
- IPCC (Intergovernmental Panel on Climate Change). 2013. *Climate Change 2013: The Physical Science Basis*. Contribution of Working Group I to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change (T.F. Stocker, D. Qin, G.-K. Plattner, M. Tignor, S.K. Allen, J. Boschung, et al., eds.). Cambridge: Cambridge University Press.
- IPCC. 2014. *Climate Change 2014: Synthesis Report*. Contribution of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change (Core Writing Team, R.K. Pachauri, and L.A. Meyer, eds.). IPCC, Geneva, Switzerland. [http://ar5-syr.ipcc.ch/ipcc/ipcc/resources/pdf/IPCC\\_SynthesisReport.pdf](http://ar5-syr.ipcc.ch/ipcc/ipcc/resources/pdf/IPCC_SynthesisReport.pdf).
- Kunkel, K. 2016. "NOAA Cooperative Institute for Climate and Satellites (NC State)." Presentation to the Committee on Enhancing the Resilience of Nation's Electric Power Transmission and Distribution System on July 11. Washington, D.C.
- Lloyds. 2013. *Solar Storm Risk to the North American Electric Grid*. <https://www.lloyds.com/~media/lloyds/reports/emerging%20risk%20reports/solar%20storm%20risk%20to%20the%20north%20american%20electric%20grid.pdf>.
- MITRE. 2011. *Impacts of Severe Space Weather on the Electric Grid*. <https://fas.org/irp/agency/dod/jason/spaceweather.pdf>.
- NASEM (National Academies of Sciences, Engineering, and Medicine). 2016. *Attribution of Extreme Weather Events in the Context of Climate Change*. Washington, D.C.: The National Academies Press.
- National Atlas and USGS. 2005. "Hurricane Hazards—A National Threat." [https://walrus.wr.usgs.gov/infobank/programs/html/factsheets/pdfs/2005\\_3121.pdf](https://walrus.wr.usgs.gov/infobank/programs/html/factsheets/pdfs/2005_3121.pdf). Accessed July 13, 2017.
- NCAR (The National Center for Atmospheric Research). 1988. "NCAR Co-Hosts Wildfire Severity and Global Climate Change Workshop." <https://opensky.ucar.edu/islandora/object/archives%3A883>. Accessed July 13, 2017.
- NOAA (National Oceanic and Atmospheric Administration). 2016. "Historical Records and Trends." <https://www.ncdc.noaa.gov/climate-information/extreme-events/us-tornado-climatology/trends>. Accessed February 28, 2017.
- NOAA and NSSL (National Severe Storms Laboratory). 2009. "Tornado Days (1990–2009)." Oklahoma Climatological Survey. [http://climate.ok.gov/index.php/climate/map/tornado\\_days\\_1990\\_2009/tornadoes\\_severe\\_storms](http://climate.ok.gov/index.php/climate/map/tornado_days_1990_2009/tornadoes_severe_storms). Accessed February 28, 2017.
- NRC (National Research Council). 2007. *Elevation Data for Floodplain Mapping*. Washington, D.C.: The National Academies Press.
- NRC. 2008. *Severe Space Weather Events—Understanding Societal and Economic Impacts: A workshop report*. Washington, D.C.: The National Academies Press.
- NRC. 2012. *Terrorism and the Electric Power Delivery System*. Washington, D.C.: The National Academies Press.
- OTA (Office of Technology Assessment). 1990. *Physical Vulnerability of Electric System to Natural Disasters and Sabotage, OTA-E-453*. Washington, D.C.: U.S. Government Printing Office.
- Parfomak, P. 2014. *Physical Security of the U.S. Power Grid: High-Voltage Transformers Substations*. <https://fas.org/spp/crs/homesec/R43604.pdf>.
- Peltier, R. 2012. "Dominion's North Anna Station Sets New Standard for Earthquake Response." *Power*, November 1. <http://www.powermag.com/dominions-north-anna-station-sets-new-standard-for-earthquake-response/?pagenum=3>. Accessed April 28, 2017.
- Petersen, M.D., M.P. Moschetti, P.M. Powers, C.S. Mueller, K.M. Haller, A.D. Frankel, Y. Zeng, et al. 2014. *Documentation for the 2014 Update of the United States National Seismic Hazard Maps*. U.S. Geological Survey, Open-File Report 2014–1091.
- Seneviratne, S.I., N. Nicholls, D. Easterling, C.M. Goodess, S. Kanae, J. Kossin, Y. Luo, et al. 2012. Changes in climate extremes and their impacts on the natural physical environment. Pp. 109–230 in *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation* (C.B. Field, V. Barros, T.F. Stocker, D. Qin, D.J. Dokken, K.L. Ebi, M.D. Mastrandrea, et al., eds.). A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change (IPCC). Cambridge: Cambridge University Press.
- Tang, B. 2008. "National Center for Atmospheric Research." <http://www.ustornadoes.com/wp-content/uploads/2014/04/brian-tang-april27-ncar.png>. Accessed July 13, 2017.
- Tippett, M.K., C. Lepore, and J.E. Cohen. 2016. More tornadoes in the most extreme U.S. tornado outbreaks. *Science* 354(6318): 1419–1423.
- UCS (Union of Concerned Scientists). 2016. "Hurricanes and Climate Change." [http://www.ucsusa.org/global\\_warming/science\\_and\\_impacts/impacts/hurricanes-and-climate-change.html#.WJS9OW8rLGg](http://www.ucsusa.org/global_warming/science_and_impacts/impacts/hurricanes-and-climate-change.html#.WJS9OW8rLGg). Accessed November 27, 2016.
- USGCRP (U.S. Global Change Research Program). 2014. "National Climate Assessment." <http://nca2014.globalchange.gov/>. Accessed July 13, 2017.
- USGS (U.S. Geological Survey). 2008. "Mount Rainier—Living Safely With a Volcano in Your Backyard." <https://pubs.usgs.gov/fs/2008/3062/fs2008-3062.pdf>.
- USGS. 2016a. "Tsunami hazards—A National Threat." <https://water.usgs.gov/edu/tsunamishazards.html>. Accessed February 28, 2017.
- USGS. 2016b. "U.S. Volcanoes and Current Activity Alerts." <https://volcanoes.usgs.gov/index.html>. Accessed February 28, 2017.
- Vastag, B. 2011. Nuclear power plant remains offline after August earthquake. *The Washington Post*, November 1.
- Wuebbles, D., G. Meehl, K. Hayhoe, T.R. Karl, K. Kunkel, B. Santer, M. Wehner, et al. 2014. CMIP5 climate model analyses: Climate extremes in the United States. *Bulletin of the American Meteorological Society* 95(4): 571–583.

# 4

## Strategies to Prepare for and Mitigate Large-Area, Long-Duration Blackouts

### INTRODUCTION

This chapter focuses on strategies that can help to avoid, prepare for, and reduce the likelihood, magnitude, and duration of large-area, long-duration outages.<sup>1</sup> Although this report is predominantly concerned with large-scale outages, many of the preventative approaches described in this chapter also decrease the likelihood of small localized outages and can help limit the spread and impact of small disruptions before major recovery efforts (see Chapter 6) are required.

This chapter concentrates on two broad aspects of improving grid resilience, considering both physical and cyber impairments. The first, planning and design, describes actions to enhance resilience that can be taken well before a potentially severe physical or cyber event occurs. The second, operations, describes how the grid is operated and strategies to enhance resilience during a severe event. Certainly there is overlap between these two, and the dividing line can blur as the planning time horizon moves closer to the real-time world of operations.

### PLANNING AND DESIGN

The electric utility industry has a long history of planning, and the present high levels of reliability attest to its success in this area. However, the majority of this planning and design work has been directed toward increasing system reliability, while focusing on designing the system for optimal operations during normal conditions and creating the ability to respond to events similar to those that have been previously encountered by grid operators. Planning and design for resilience is different, with challenges that touch on essentially all aspects of the electric grid.

A resilient design requires a holistic consideration of both the resilience of the individual components that comprise

modern electric grids and the resilience of the system as a whole. There is, of course, overlap between the two: system resilience can be enhanced by improved component resilience. However, improved resilience also involves consideration of the system as a whole, including not just the electric infrastructure itself, but also the interdependent infrastructures such as natural gas infrastructure, support infrastructure for the supply of other key inputs, and the commercial communications systems used in operating the grid. Last, improved resilience requires regulatory consideration of how upgrades will be funded.

### Component Hardening and Physical Security

Creating reliable and secure components, investing in system hardening, and pursuing damage prevention activities are all strategies that improve the reliability of the grid and likewise play a role in preventing and mitigating the extent of large-area, long-duration outages. Utilities are generally aware of local hazards; however, these hazards may change over time, and utilities may not be aware of the compound vulnerabilities that become increasingly possible. Strategies used to address these hazards include appropriate design standards, siting methods, construction, maintenance, inspection, and operating practices. For example, a transmission line traversing high mountains must be designed for heavy ice loading, which may not be a design consideration for infrastructure located in desert environments. Design considerations for generation facilities, substations, transmission lines, and distribution lines frequently include environmental conditions such as extreme heat, cold, ice, and floods among other known threats. Utilities have less experience in design and hardening for uncommon threats such as geomagnetic disturbance (GMD) or electromagnetic pulse (EMP); nonetheless, these have been the focus of increasing attention and strategies to reduce system vulnerability.

Utility investment in system hardening is typically informed by a risk-based cost-performance optimization that strives to be economically efficient by investing in

<sup>1</sup> Such events overlap with what the North American Electric Reliability Corporation (NERC) calls a “severe event,” defined as an “emergency situation so catastrophic that complete restoration of electric service is not possible” (NERC, 2012a).

mitigation strategies with the greatest reduction in risk at the lowest cost (Figure 4.1). In principle, an infinite amount of money could be spent hardening and upgrading the system with costs passed on to ratepayers or taken from shareholder returns. However, utilities and their regulators (or boards) are typically conservative in these investments. All mitigation strategies have cost-performance trade-offs, and it may be difficult to estimate the actual reduction in risk or improvement in resilience associated with a specific action. In most cases, an electricity system that is designed, constructed, and operated solely on the basis of economic efficiency to meet standard reliability criteria will not be sufficiently resilient. If some comprehensive quantitative metric of resilience becomes available, it should be combined with reliability metrics to select a socially optimal level of investment. In the meantime, decision makers must employ heuristic procedures to choose a level of additional investment they believe will achieve a socially adequate level of system redundancy, flexibility, and adaptability.

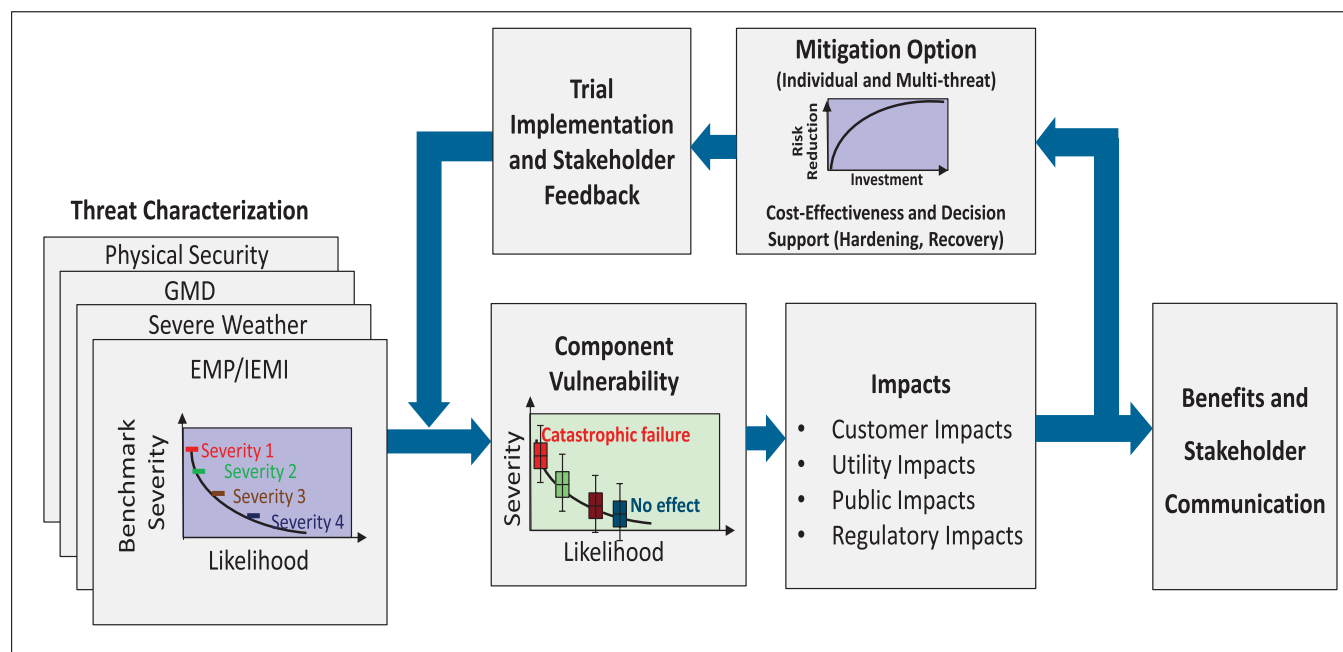
**Finding:** Design choices based on economic efficiency using only classical reliability metrics are typically insufficient for guiding investment in hardening and mitigation strategies targeted toward resilience. Such choices will typically result in too little attention to system resilience. If adequate metrics for resilience are developed, they could be employed to achieve socially optimal designs. Until then,

decision makers may employ heuristic procedures to choose the level of additional investment they believe will achieve socially adequate levels of system redundancy, flexibility, and adaptability.

Hardening and mitigation strategies can improve electricity grid reliability and resilience, and utilities routinely employ many techniques when deemed cost appropriate. Common examples are described in the following paragraphs.

### Vegetation Management

Many outages, particularly those in the distribution system, are caused by trees and vegetation that encroach on the right-of-way of power lines. Overhead transmission lines are not directly insulated and instead require minimum separation distances for air to provide insulation. If trees or objects are allowed to get too close and draw an arc, short circuits of the energized conductor can result. When they are heavily loaded, transmission line conductors heat up, expand, and sag lower into the right-of-way, which increases the likelihood of a fault at times of peak transmission loading. Therefore, inadequate vegetation management in transmission line rights-of-way is a common cause of blackouts. On the lower-voltage distribution system, separation requirements are much smaller, and line sag is less of a consideration. However, during high wind or icy conditions, falling trees



**FIGURE 4.1** The process of considering and mitigating individual component vulnerability based on cost-performance optimization.

NOTE: GMD, geomagnetic disturbance; EMP, electromagnetic pulse; IEMI, intentional electromagnetic interference.

SOURCE: Courtesy of the Electric Power Research Institute. Graphic reproduced by permission from the Electric Power Research Institute from presentation by Rich Lordan to the NCSL-NARUC Energy Risk & Critical Infrastructure Protection Workshop, Transmission Resiliency & Security: Response to High Impact Low Frequency Threats. EPRI, Palo Alto, Calif.: 2016.

and limbs can either create a short circuit or tear down the wires themselves. This can be extremely hazardous when the energized wires are in close proximity to people. So while there are different vegetation management practices for transmission (clearing vegetation below the wires) and distribution (clearing vegetation from around and above the wires), vegetation management is a key factor that influences the reliability of the transmission and distribution (T&D) system. Following the widely publicized blackout of August 14, 2003, new national standards for vegetation management of transmission lines were implemented. However, the vegetation management practices for distribution utilities vary dramatically, influenced by a variety of factors including geography, public sentiment, and regulatory encouragement.

### Undergrounding

Undergrounding of T&D lines is often more expensive than building aboveground infrastructure. Outside of dense urban environments, T&D assets are typically not installed underground unless land constraints, aesthetics, or other community concerns justify the cost. Undergrounding protects against some threats to the resilience of the electric grid, such as severe storms—a leading cause of outages—but it does not address all threats (e.g., seismic or flooding) and may even make recovery more challenging. Furthermore, undergrounding may be impractical in some areas, based on geologic or other constraints (e.g., areas with a high water table). Therefore, the decision of whether or not to underground T&D assets varies considerably based on local factors; while undergrounding may have resilience benefits in some circumstances, it does not offer a universal resilience benefit.

### Reinforcement of Poles and Towers

Building the T&D network to withstand greater physical stresses can help prevent or mitigate the catastrophic effects of major events. Structurally reinforcing towers and poles (referred to as robustness) is more common in areas where heavy wind or ice accumulations are possible, but the degree to which they are reinforced presents a cost trade-off with clear resilience implications.

### Dead-End Structures

To minimize cost, transmission towers are often designed to support only the weight of the lines, with lateral support provided by the lines themselves, which are connected to adjacent towers. Thus, if one tower is compromised, it can potentially create a domino effect whereby multiple towers fail. To limit this, utilities install dead-end structures with sufficient strength to stop such a domino effect. However, there is a cost trade-off associated with how often such structures should be installed (e.g., changing the spacing

from having one dead-end structure every 4 miles versus one dead-end structure every 10 miles).

### Water Protection

Flooding is often a greater concern for substations and generation plants than transmission and distribution lines, and storm surge is particularly challenging for some coastal assets. When siting new facilities, it is possible to avoid low lying and flood prone areas. There are, however, many legacy facilities located in high hazard areas. Given that much of the population lives in coastal areas, it is impossible to address this risk completely through siting alone. Common techniques include installing dikes and/or levees, if land permits, or elevating system components above flood levels, which can be expensive when retrofitting legacy facilities.

### Emerging Strategies for Geomagnetic Disturbance and Electromagnetic Pulse

There are various electromagnetic threats to the power system, including GMD (naturally occurring) and EMP (man-made). Both of these threats have resilience considerations at the component level and from a system-wide perspective. While they have different mechanisms of coupling to the grid and inducing damage, they are similar in that they can damage high-value assets, such as transformers. The EMP threat is unique in that it can directly incapacitate digital equipment such as microprocessors and integrated circuits that are not military hardened. NERC has new planning requirements for mitigating GMD (NERC, 2016a), and various commissions (e.g., the Commission to Assess the Threat to the United States from Electromagnetic Pulse [EMP] Attack<sup>2</sup>) have explored the degree to which it is appropriate to harden civilian infrastructure to address the EMP threat.

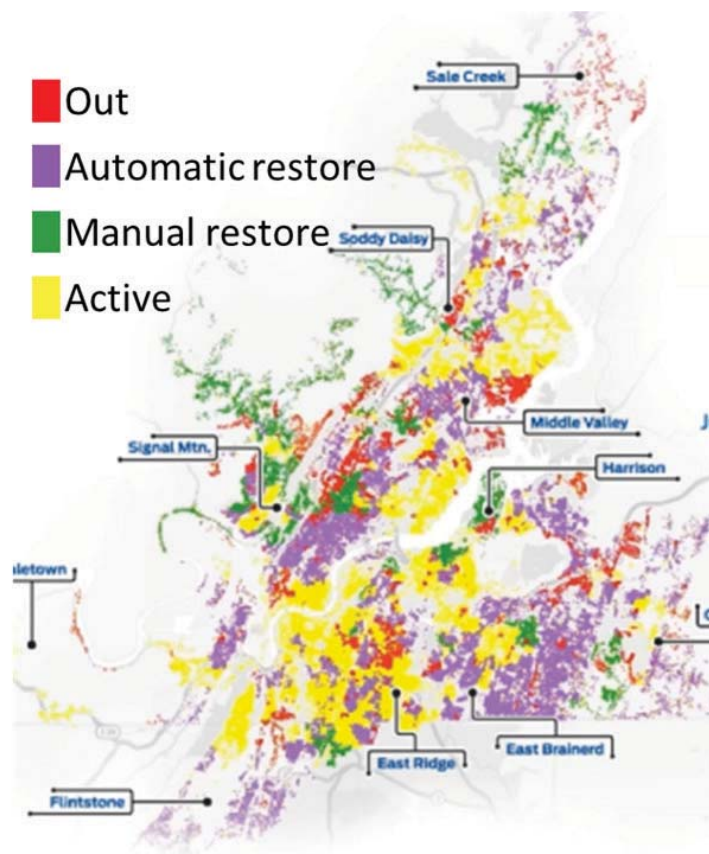
### Physical Security

The immense size and exposed nature of electricity infrastructure makes complete physical protection from attacks impossible; thus, there is a spectrum of physical security practices employed across the grid. Utilities selectively protect critical system components, and NERC standard CIP-014-2 (NERC, 2014a) is enforced on the transmission system. Distribution systems are outside the scope of NERC jurisdiction. Because many generation facilities are staffed, they are relatively well protected. Additional federal requirements apply to protecting nuclear and other key assets, such as federally owned dams. Other assets essential to the operation of the system, such as control centers, can resemble bunkers and are well guarded. Many substations are

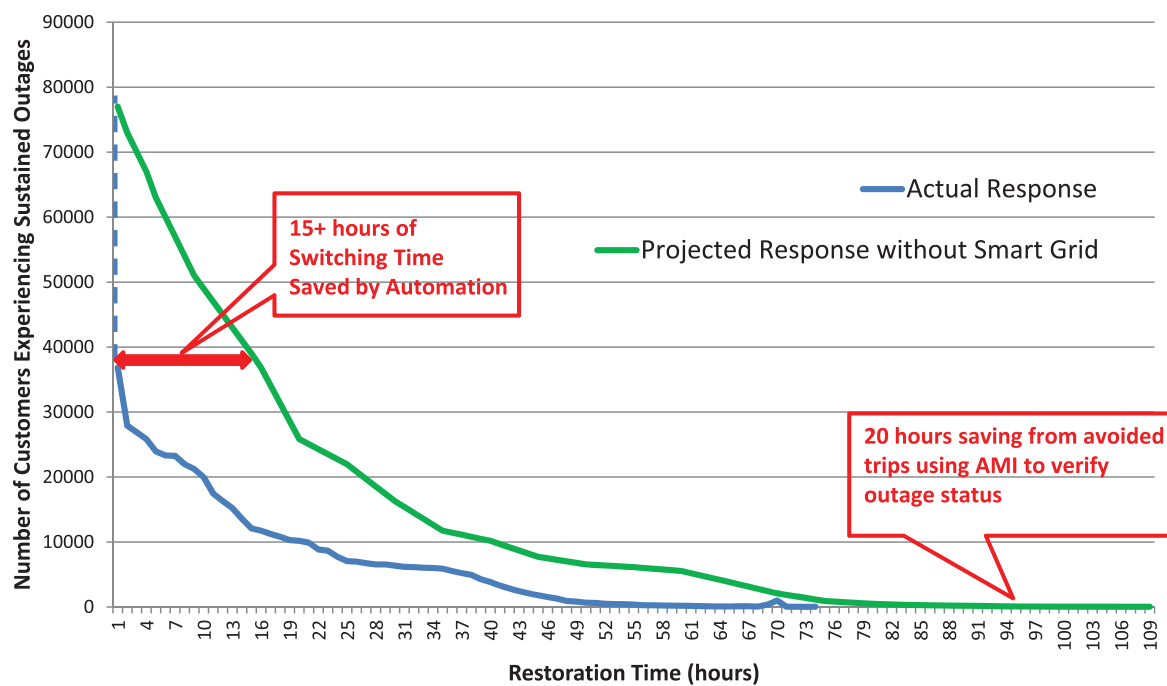
<sup>2</sup> Reports from the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack can be found at <http://www.empcommission.org>, accessed August 2, 2017.



(A)



(B)



**FIGURE 4.2** (A) Following a major storm that disrupted service on many distribution circuits operated by Chattanooga Electric Power Board, automatic reconfiguration prevented outages for many customers (purple) and significantly reduced the number of circuits requiring manual repairs (green); and (B) such automation has greatly reduced the number of customer-hours (area under the curve) of outage experienced. NOTE: AMI, advanced metering infrastructure. SOURCE: Glass (2016).



less protected and have only surveillance, locks, and other deterrents. However, historical events such as the Metcalf incident (see Box 3.1) and a recent “white hat” break-in and hack of a utility shared on YouTube call attention to the limitations of these strategies. Alternative strategies include redesigning substation layout to minimize exposure, deploying barriers, protecting information about the location of critical components, and improving adoption of best practices and standards (ICF, 2016). Examples of these practices learned from the Metcalf incident include greater emphasis on outside-the-fence measures, including camera coverage, lighting, and vegetation clearing.

### Distribution System Resilience

As noted in Chapter 2, the wires portion of the electric grid is usually divided into two parts: the high-voltage transmission grid and the lower-voltage distribution system. The transmission system is usually networked, so that any particular location in the system will have at least two incident transmission lines. The advantage of a networked system is that loss of any particular line would not result in a power outage. In contrast, the typical distribution system is radial (i.e., there is just a single supply), although networked distribution systems are often used in some urban areas (NASEM, 2016a). Most aspects of resilience to severe events ultimately involve the transmission system; however, improved distribution system resilience can play an important role.

There is wide variation in the level of technological sophistication in distribution systems. The most advanced distribution utilities have dedicated fiber-optic communications networks, are moving away from the traditional radial feeder design toward more networked architectures, and have sectionalizing switches that allow isolation of damaged components. In response to damage on a distribution circuit, these systems automatically reconfigure the distribution network to minimize the number of customers affected. In one notable example, shown in Figure 4.2 and detailed in Box 4.1, the Chattanooga Electric Power Board (EPB) installed significant distribution automation technology with a \$111 million grant from the Department of Energy (DOE) through its Smart Grid Investment Grant program (authorized by the 2009 American Recovery and Reinvestment Act). The sophisticated and extensive project entailed installing a dedicated fiber-optics communications system, smart distribution switches, advanced metering infrastructure, and other equipment to automate restoration (DOE, 2011). It decreased restoration times for EPB’s customers, increased savings to EPB, and demonstrated possibilities for other utilities to emulate. However, pursuing a closed-loop fiber-optic system may be a challenge in other utility service areas that are larger geographically and in terms of population. While fiber-optic communication offers an advantage, it is not required to integrate the other technologies used at EPB. However, the deployment of a fiber-optic system lays the foundation

#### BOX 4.1 Financial and Operational Benefits of Distribution Automation to Chattanooga Electric Power Board

**Resilience and Reliability:** The installed fiber-optic network allows EPB to manage a greater number of restoration crews following a storm event and, based on a limited time frame, improve its system average interruption duration index (SAIDI) and system average interruption frequency index (SAIFI) reliability metrics (Glass, 2016; Wade, 2016).

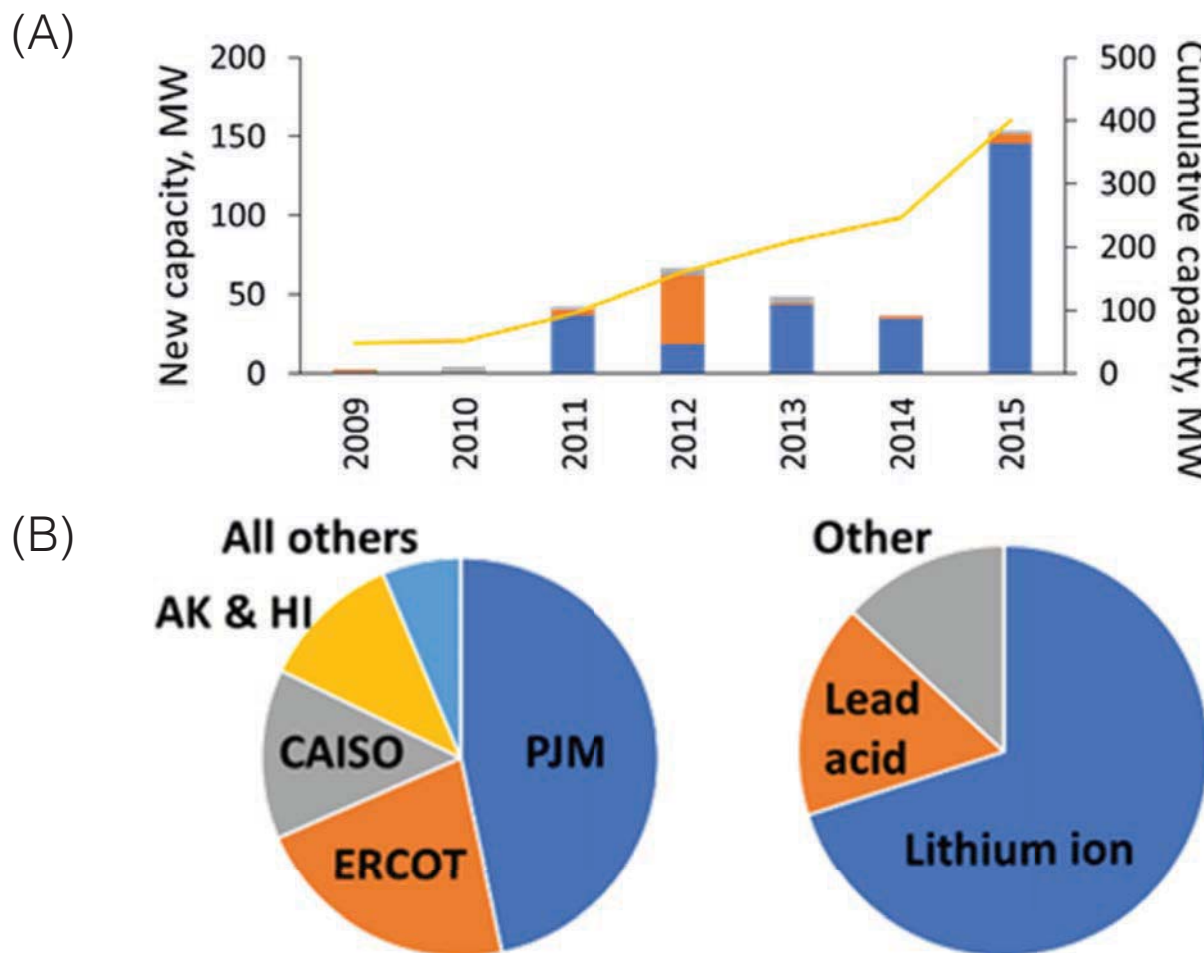
**Financial Savings:** Annual savings of \$200,000 are due to decreased dispatch of restoration crews, \$2.5 million from automated meter reading and remote disconnect, and \$2.7 million in energy demand savings from demand response and voltage control. Taken together, EPB saves nearly \$5.5 million as a result of its fiber-optic and automation technologies (Glass, 2016).

for technologies that result in very high data exchange rates, such as phasor measurement units (PMUs), and offers the ability to provide broadband access to the community.

A distribution fault anticipation application based on “waveform analytics” (Wischkaemper et al., 2014, 2015) is another example of a technology that could be applied today. The key idea behind this approach is to utilize fast sensing of the distribution voltages and currents to detect precursor waveforms, which indicate that a component on a distribution circuit will soon fail. This is in contrast to the traditional approach of waiting for the component to fail and cause an outage before doing repairs. Examples of problems that can be detected by such pre-fault waveform analysis include cracked bushings, pre-failure of a capacitor vacuum switch, fault-induced conductor slap (in which a fault current in the distribution circuit induces magnetic forces in another location, causing the conductors to slap together), and pre-failure of clamps and switches.

**Finding:** While many distribution automation technologies are available that would enhance system resilience, their cost of deployment remains a barrier, particularly in light of challenges in monetizing the benefits of such installations.

**Recommendation 4.1:** Building on ongoing industry efforts to enhance system resilience, the Department of Energy and utility regulators should support a modest grant program that encourages utility investment in innovative solutions that demonstrate resilience enhancement. These projects should be selected to reduce barrier(s) to entry by improving



**FIGURE 4.3** (A) Installations of utility-scale battery storage have increased substantially over the past 5 years, (B) although growth is concentrated in a few areas and dominated by lithium-ion chemistries.

NOTE: CAISO, California Independent System Operator; ERCOT, Electric Reliability Council of Texas.

SOURCE: Data from Hart and Sarkissian (2016).

regulator and utility confidence, thereby promoting wider adoption in the marketplace.

### Utility-Scale Battery Storage

Utility-scale battery storage is a relatively new tool available to operators to manage power system stability, which can potentially help prevent or mitigate the extent of outages. Of course even large batteries can only supply power for periods of hours, but such systems have value in other ways. They can be used to dispatch large amounts of power for frequency regulation, potentially preventing propagation of system disturbances, and provide additional flexibility for managing stability in lieu of demand response or load shedding. Installations of large utility-scale batteries (as opposed to behind-the-meter batteries) have increased significantly in several regions of the United States over the past 5 years. The DOE Global Energy Storage Database has information

on more than 200 utility-scale battery projects in the United States, with more than 400 MW installed or approved capacity by the end of 2015 (Figure 4.3) (Hart and Sarkissian, 2016). This data set may underestimate such storage capacity.<sup>3</sup> Other areas leading installation are in the Electric Reliability Council of Texas (ERCOT) and in California, driven largely by state policies (NREL, 2014). The small (relative to the scale of the three North American interconnections) Railbelt Electric System in Alaska was an early adopter (2003) of utility-scale battery energy storage, in part owing to instability challenges associated with operating a small, low-inertia “islanded” grid. Most utility-scale batteries on the grid employ lithium-ion chemistry and are used primarily for power conditioning and, to a lesser extent, for peak load management. Lithium-ion chemistry using existing electrolytes

<sup>3</sup> The committee believes there is approximately 400 MW capacity installed in the PJM service territory alone.

is not ideal for bulk storage of electricity from large-scale, variable renewable generation sources, but alternative battery chemistries have yet to reach the cost, performance, and manufacturing scale to impact utility operations.

### **Distributed Energy Resources**

Distributed energy resources (DERs)—including distributed generation from photovoltaics, diesel generators, small natural gas turbines, battery storage, and demand response—have the potential to help prevent the occurrence of large-area, long-duration outages as well as to provide local power to critical services during an outage. In California, for example, storage aggregators are contracting with utilities to provide tens of MW of storage capacity—alongside 70 MW of utility-scale storage—to help manage local resource adequacy and reliability following the closure of the Aliso Canyon facility (see Box 4.2). However, the reliability and resilience benefits of DERs to the bulk power system vary significantly, based on their technical characteristics and capacities as well as their location and local grid characteristics. Historically, DER adoption has

been driven by environmental considerations and consumer preferences; only recently has resilience become an explicit design consideration. The greatest resilience benefits can be realized through coordinated planning and upgrading of T&D systems, as well as by providing operators the ability to monitor and control the operating characteristics of DERs in real time and at scale. This may require changes to technical standards, regulations, and contractual agreements.

Strategically placed DERs (that are visible to and controllable by utilities) not only provide local generation at the end of vulnerable transmission lines, but also can be operated to relieve congestion and potentially avoid the need for new transmission infrastructure. Thus, some of the early applications of DERs for enhanced resilience were motivated by local system concerns—in locations with constraints on transmission expansion or at the end of lines that are known to be problematic.

### **Inverter Standards for Increased Visibility and Control**

At current levels of installation (relatively low except in certain areas such as Hawaii), DERs are not likely to be used

## **BOX 4.2**

### **Examples of Electric System Vulnerability to Disruptions in Natural Gas Infrastructure**

#### **February 2011 Texas Freeze**

Abnormally cold temperatures across Texas and the southwestern United States caused many natural gas well heads to freeze, which in turn resulted in curtailment of natural gas deliveries to end-use customers and, to a lesser extent, natural gas fired power plants. The cold weather caused 193 power plants (with cumulative load of nearly 30,000 MW) in ERCOT to fail to start or to be de-rated because of frozen equipment, blade icing, and low temperature cutoff limits. At the worst point in the event, one-third of the total ERCOT generator fleet was unavailable. System operators resorted to shedding load and instituted rolling blackouts to prevent an ERCOT-wide uncontrolled blackout. Although electricity–natural gas interdependency was not the primary cause of lost electric load or curtailed natural gas deliveries, the growing interdependency did contribute to the problem (NERC, 2011).

#### **January 2014 Polar Vortex**

In January 2014, a mass of cold air moved south across much of the country, plunging the Midwest, Northeast, and Southeast into temperatures 20° to 35° colder than average. The cold snap resulted in above average demand for electricity and natural gas for home heating. Many natural gas power plants were unable to operate as natural gas deliveries were curtailed, and grid operators had to resort to shedding interruptible load to maintain service. Less than 50 MW of firm load was shed over several days, and the event was handled effectively in part because of training and preparation. However, the event focused attention on the vulnerability associated with increasing reliance on natural gas for electricity restoration. Following the 2014 Polar Vortex, NERC made a number of recommendations for operators to increase awareness and coordination with natural gas suppliers, markets, and regulators (NERC, 2014b).

#### **October 2015 Aliso Canyon Storage Facility Closure**

A major gas leak was detected in the Aliso Canyon natural gas storage facility in October 2015, resulting in the facility's closing in early 2016. As the second largest natural gas storage facility in the United States, Aliso Canyon supplied gas to 18 power plants in the Los Angeles area with a total generation capacity near 10,000 MW (NERC, 2016b). Analysis suggests that closure of the facility may have significant electricity system reliability impacts, as well as curtailment of gas deliveries, in both summer and winter (CEC, 2016). In combination with the 2014 Polar Vortex, the Aliso Canyon blowout prompted the industry to undertake additional planning and risk mitigation strategies to reduce the likelihood that outages will result from natural gas system constraints.

explicitly for the purpose of preventing or mitigating large-scale outages. Nonetheless, as DER installations continue to grow, it may become possible to coordinate their dispatch to help prevent outages (i.e., maintain system stability) and to expedite restoration (as described in Chapter 6). However, realizing these system benefits would require that system operators—whether distribution utilities or independent parties—have visibility and an appropriate level of control over the majority of DERs in a region.

This will require changes in interconnection standards, notably regarding inverters that are the interface between many types of DERs and the distribution system. In the past, these standards, which are under revision as of this writing, have required that DERs disconnect from the grid under fault conditions. This is undesirable behavior because it can jeopardize system stability under significant DER penetration levels. In the revised standards (IEEE, 2017), inverters will be required to ride through grid events, and they will have the ability to provide voltage and frequency regulation. Future inverters will provide operators with updated information on DER performance (e.g., generation level, state of charge), who could in turn actively utilize these resources in running the grid (e.g., when implementing adaptive islanding or intelligent load shedding schemes).

A non-exhaustive list of advanced inverter functionalities that could help prevent or mitigate outages, if they can be leveraged at scale, includes the following:

- *Frequency-watt function.* Adjusts real power output based on service frequency and can aid in frequency regulation during an event.
- *Volt-var and volt-watt function.* Adjusts reactive and/or real power output based on service voltage; this is necessary to maintain distribution feeder voltages within acceptable bounds when DER penetration is high, but it could also be used for transmission-level objectives.
- *Low/high voltage and frequency ride-through.* Defines voltage and frequency ranges for the inverter to remain online during a disturbance, which becomes a key feature at high DER penetration levels.
- *DER settings for multiple grid configurations.* Enables a system operator to provide a DER with alternate settings, which may be needed when the local grid configuration changes (e.g., during islanding or circuit switching).

**Finding:** DERs have a largely untapped potential to improve the resilience of the electric power system but do not contribute to this inherently. Rather, resilience implications must be explicitly considered during planning and design decisions. In addition, the possibility exists to further utilize DER capabilities during the operational stage.

**Recommendation 4.2:** The Department of Energy and the National Science Foundation, in coordination with state

agencies and international organizations, should initiate research, development, and demonstration activities to explore the extent to which distributed energy resources could be used to prevent large-area outages. Such programs should focus on the technical, legal, and contractual challenges to providing system operators with visibility and control over distributed energy resources in both normal and emergency conditions. This involves interoperability requirements and standards for integration with distribution management systems, which are ideally coordinated at the national and international levels.

### Interconnected Electric Grid Modeling and Simulation

From the start of the power industry in the 1880s, modeling and simulation have played a crucial role, with much expertise gained over this time period. Over the past 60 years or so, much of this expertise has been embedded in software of increasing sophistication, with power-flow, contingency-analysis, security-constrained optimal power-flow, transient-stability, and short-circuit analysis some of the key modeling packages (NASEM, 2016b). Modeling and simulation occur on time frames ranging from real time, in the case of operations, to looking ahead for multiple decades when planning high-voltage transmission line additions.

While the tools are well established for these traditional applications, enhancing resilience presents some unique challenges. First, multidimensional modeling is needed because severe events are likely to affect not just the electric grid, but also other infrastructures. Second, in order to enhance resilience, simulations should be specifically designed to consider rare events that severely stress the grid. Many rare high-impact events will stress the power grid in new and often unexpected ways; as a consequence, most will also likely stress the existing power system modeling software. The degree of power system impact often requires detailed modeling of physical and/or cyber systems associated with the initiating event. For example, correctly modeling the impacts of large earthquakes requires coupled modeling between the power grid and seismic simulations (Veeramany et al., 2016). This requires interdisciplinary collaboration and research between power engineers and people from a potentially wide variety of different disciplines. On the cyber side, for example, one must be able to correctly model the occurrence, nature, and impact of a large-scale distributed cyber attack like the one in Ukraine in 2015.

Because such events are rare, there is typically little or no historical information to accurately quantify or characterize the risk: some of the more extreme events could be considered extreme manifestations of more common occurrences (NASEM, 2016b). Thus, a large-scale attack could be considered a more severe manifestation of the more regular disturbances (such as those due to the weather). However, others would be more novel. As an example, consider the modeling and simulation work being done to



study the impact of GMD on the power grid. GMDs, which are caused by coronal mass ejections from the sun, cause low frequency ( $\ll 0.1$  Hz) variations in the earth's magnetic field. The changing magnetic field can then induce electric fields on the earth's surface that cause quasi-direct current geomagnetically induced currents to flow in the high-voltage transmission system, potentially causing saturation in the high-voltage transformers. A moderate GMD, with a peak electric field estimated to be about 2 V/km, caused a blackout for the entire province of Québec, Canada, in 1989 (Boteler, 1994), while much larger GMD events occurred in North America in 1859 and 1921.

As noted by Albertson et al. (1973), the potential for GMD to interfere with power grid operations has been known at least since the early 1940s. However, power grid GMD assessment is still an active area of research and development; much of that work has occurred in the past few years through interdisciplinary research focusing not just on the power grid, but also on the sun, the earth's upper atmosphere, space weather hazards, and the earth's geophysical properties. The assumptions on modeling the driving electric fields in software have evolved from a uniform electric field (NERC, 2012b); to scaled uniform direction electric fields, based on ground conductivity regions (based on one-dimensional earth models) (NERC, 2016a); to varying magnitude and electric fields, based on three-dimensional earth models using recent National Science Foundation Earthscope results (Bedrosian and Love, 2015). Over the past few years, GMD analysis has been integrated into commercial power system planning tools including the power flow (Overbye et al., 2012) and transient stability analysis software (Hutchins and Overbye, 2016).

Determining the magnitudes of the severe events to model can be challenging since there is often little historical record. This was highlighted in 2016 by the Federal Energy Regulatory Commission (FERC) in their Order 830,<sup>4</sup> which directed NERC to modify its Standard TPL-007-1 GMD benchmark event so as not to be solely based on spatially averaged data. The challenges of using measurements of the earth's magnetic field variation over about 25 years to estimate the magnitude of a 100-year GMD are illustrated by Rivera and Backhaus (2015). Determining the scenarios to consider for human-caused severe events, such as a combined cyber and physical attack, are even more challenging.

**Finding:** Enhancing power grid resilience requires being able to accurately simulate the impact of a wide variety of severe physical events and malicious cyber attacks on the power grid. Usually these simulations will require models for either coupled physical and cyber infrastructures or physical systems. There is a need both for basic research on the nature of these simulations and applied work to develop adequate simulations to model these severe events and malicious cyber attacks.

**Recommendation 4.3:** The National Science Foundation should continue to expand support for research looking at the interdisciplinary modeling and mitigation of power grid severe events. The Department of Energy should continue to support research to develop the methods needed to simulate these events.

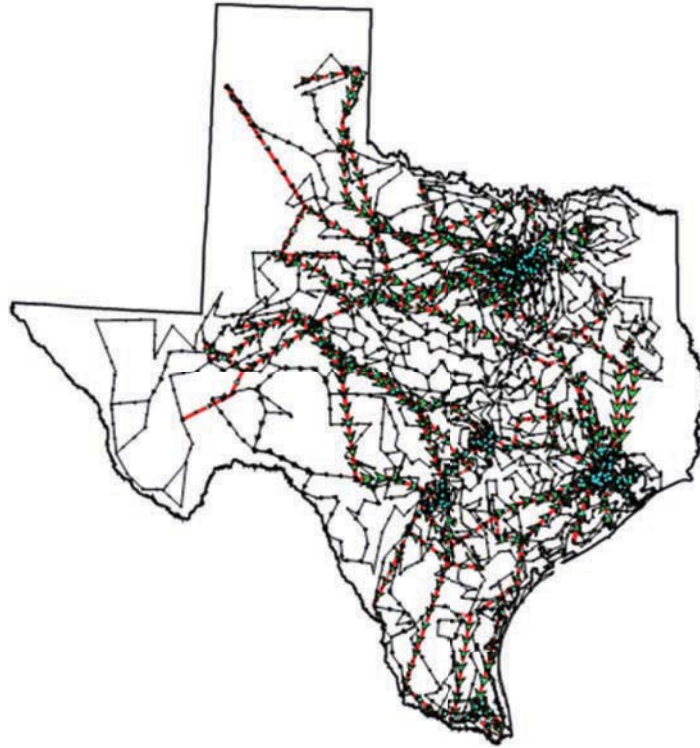
A key driver for the research and development of simulation tools for improved resilience is access to realistic models of large-scale electric grids and their associated supporting infrastructures, especially communications. Some of this information was publicly available in the 1990s, but, as a result of the Patriot Act of 2001, the U.S. electric power grid is now considered critical infrastructure, and access to data has become much more restricted. While some access to power grid modeling data is available under non-disclosure agreements, these restrictions greatly hinder the exchange of the models and results needed for other qualified researchers to reproduce the results. This need is particularly acute for resilience studies, in which models need to be shared among researchers in a variety of fields for interdisciplinary work.

A solution that protects critical infrastructure information is to create entirely synthetic models that mimic the complexity of the actual grid but contain no confidential information about the actual grid. Such models are now starting to appear, driven in part by the DOE Advanced Research Projects Agency-Energy Grid Data program (ARPA-E, 2016), which is focused on developing realistic, open-access power grid models primarily for use in the development of optimal power flow algorithms. A quite useful characteristic of such synthetic models would be to include realistic geographic coordinates in order to allow the coupling between the power grid and other infrastructures or the actual geography. Birchfield et al. (2016) suggest using an electric load distribution that matches the actual population in a geographic footprint, public data on the actual generator locations, and algorithms to create an entirely synthetic transmission grid. As an example, Figure 4.4 shows a 2000-bus entirely synthetic network sited geographically in Texas. The embedding of geographic coordinates with the existing Institute of Electrical and Electronics Engineers' 145-bus test system is used by Veeramany et al. (2016) to present a multi-hazard risk-assessment framework for study of power grid earthquake vulnerabilities.

While there has been some progress in creating synthetic models for the physical side of the electric grid, there has been very little progress in creating realistic models for the communications that support grid operations, both to represent its complexity and extent and to represent its coupling with the physical portion of the grid. Such models are necessary to understand the overall resilience of the power grid. Without such models, it is impossible to understand the impact of a cyber attack on the physical portion of the grid and hence its ability to deliver power despite a cyber attack.

<sup>4</sup> 156 FERC ¶ 61,215.





**FIGURE 4.4** 2000-bus synthetic network sited in Texas. The red lines show 345 kV transmission lines, the black lines show 115 kV lines, and the green arrows show the flow of power from the generators to the loads.

SOURCE: © 1969 IEEE. Reprinted, with permission, from *Power Systems, IEEE Transactions on Grid Structural Characteristics as Validation Criteria for Synthetic Networks*.

**Finding:** A key objective for research and development of simulation tools for improved resilience is shareable access to realistic models of large-scale electric grids, considering both the grid's physical and cyber infrastructure and, equally important, the coupling between the two infrastructure sides. Because the U.S. power grid is considered critical infrastructure, such models are not broadly available to the power systems research community. Therefore, there is a need to develop synthetic models of the power grid physical and cyber infrastructure that match the size and complexity of the actual grid but contain no confidential information and hence can be fully publicly available.

**Recommendation 4.4:** The Department of Energy should support and expand its research and development on the creation of synthetic power grid physical and cyber infrastructure models. These models should have geographic coordinates and appropriate cyber and physical model detail to represent the severe events needed to develop algorithms to model and enhance resilience.

### Interconnected Electric Grid Planning

Planning for resilience requires providing sufficient redundancy in generation, transmission, and distribution capacity. Current reliability standards issued by NERC (that

are mandatory for operators of the bulk electricity system) require that the transmission system have enough redundant paths to withstand an outage by one major line or other important component (NERC, 2005). In most cases, the transmission system can continue operating with the loss of several transmission lines. At the distribution level, some state public utility commissions provide performance-based incentives that encourage distribution utilities to improve reliability metrics such as SAIDI and SAIFI, although these measures do not typically include outages associated with major events. Although NERC standards have largely been effective in addressing credible contingencies and have been recently expanded to include consideration of extreme events,<sup>5</sup> designing the grid to ride through catastrophic events such as major storms and cyber attacks pushes their limit. Furthermore, designing and building the system to withstand such major events is expensive, and while the electricity system is designed to be economically efficient (subject to reliability-based constraints such as adequacy requirements in design and operational contingency requirements in operation), additional analyses and changes in

<sup>5</sup> NERC TPL-001-4 requires studies to be performed to assess the impact of the extreme events; if the analysis concludes there is a cascading outage caused by the occurrence of extreme events, an evaluation of possible actions designed to reduce the likelihood or mitigate the consequences of the event(s) must be conducted (NERC, 2005).

planning, operational, and regulatory criteria may be needed to build incentives to design, plan, and operate the system to consider resilience in a cost-effective manner. Pushed too far, traditional strategies to make the system more robust can become cost-prohibitive, so planning and designing for graceful degradation and rapid recovery has become increasingly important for utilities.

With respect to transmission system level generation planning, the reliability standard followed in North America is a loss of load probability (LOLP) of 1 day in 10 years—enough generation capacity available to satisfy the load demand 99.97 percent of the time. If one can predict the maximum yearly load demand over many years, and good statistics of the central generator outage rates are available, one can calculate the schedule and amount of new generation capacity construction to meet this level of reliability.

As growing amounts of intermittent solar power have been added to distribution systems, the central plant generator models used in the traditional generation planning studies may be inadequate. The availability statistics were either unavailable or inadequate as the technologies were evolving. If the availability of demand curtailment, which is the same as generation availability, is also considered, the model for that will again be different, as this is dependent on factors other than weather. Finally, the addition of storage requires models that are even more complicated, as these can behave as either loads or generation with their own optimal charge/discharge schedules.

Although the generation planning criterion of the LOLP being 1 day in 10 years assures that the available generation capacity exceeds the load demand, the process ignores whether the transmission grid can move the generation to the load centers. The transmission planning process assures this by running power flow and transient stability studies on scenarios of extreme loading of the transmission grid. The planning criterion is that the system would operate normally (i.e., without voltage and loading violations) even if one major piece of equipment (e.g., line, transformer, generator) is lost for any reason—this is known as the “N-1” criterion.<sup>6</sup> Note that this is a worst case deterministic criterion, not a probabilistic criterion like LOLP; this is because no one has yet found a workable stochastic calculation that can compute the probability of meeting all the operational constraints of the grid.

These generation planning requirements work well for scenarios where there are a few central generator stations but if meeting the generation reliability requires the availability of the DERs on the distribution side (including demand and storage management), then it is not enough to run studies on only the transmission system. On the other hand, modeling

the vast numbers of distribution feeders into the contingency analysis studies would increase the model sizes by at least one magnitude. Even though this may not pose a challenge to the new generation of computers, it does pose a huge challenge to the present capabilities of gathering, validating, exchanging, and securing the model data.

The decision to invest in new generation, transmission, and distribution is more impacted by cost considerations where reliability objectives are otherwise being met. The least cost consideration must take into account not just the capital cost, but also the operational cost over the lifetime of the generation, transmission, or distribution. This cost optimization process has to include the operational scenarios over several decades, resulting in a dynamic optimization.

A major procedural hurdle has been the fact that generation (and even transmission, which is regulated) can be built by third parties whose optimal decision may or may not coincide with the optimal decision for the whole system. This multi-party decision making has essentially made the process much more difficult, and there is concern that the present decision making is too fragmented to guarantee the needed robustness of the future grid.

It is difficult enough to include all of the control and protection that is part of the grid today, but the use of distributed generation, demand response, and storage will require much more control and protection. Moreover, the rapid deployment of better measurement (advanced metering infrastructure, distribution management systems, and phasor measurement units) and communication (fiber optics) technologies are enabling a new class of control and protection that are not yet embedded into commercial-grade simulation packages.

### **Architectural Strategies to Reduce the Criticality of Components**

A reliable system includes reliable components and a system architecture design that reduces the criticality of individual components needed to maintain grid functionality. A redundant and diverse architecture can enhance resilience of the system by reducing the dependencies on single components and how they contribute to the overall system objectives. Considerations of cascading failures, fault tolerant and secure system design, and mutual dependencies are important to develop resilient architectures. While many design characteristics of the modern power grid employ these concepts, it is important to improve resilient architecture design principles to enhance the capability of the system and to have a high degree of operational autonomy under off-normal conditions.

Historically, one of the primary means of achieving system resilience in the event of accidental component failure is through redundancy. This approach has been adopted by the electricity industry since its inception and has served

<sup>6</sup> The N-1 criterion, referring to surviving the loss of the single largest component, is shorthand for a more complex set of NERC standards that specify the analysis of various categories of “credible contingencies” and acceptable system responses.

the customers well. For particularly important components or subsystems, this redundancy can also include diversity of design so as to prevent common mode failures or deliberate attacks from compromising both the primary and secondary components. Both redundancy and diversity in design are often employed in communication networks.

In addition, there is a need to design systems with insights provided by simulation of cascading failure sequences, so that technical or procedural countermeasures to thwart cascading failure scenarios can be applied. This preemptive analysis (and configuring the system to avoid conditions where cascading failure is a credible outcome) is particularly important because the speed of cascading failure sequences can often exceed the capability of automatic control responses, especially when the wide-area nature of the grid, and inherent communication delays, are taken into account.

One approach of resilient system design is to install controls that respond appropriately to limit the consequences or even stop a cascading failure sequence, regardless of the specific scenario that initiated the event. Thus, the system remains resilient even if events occur that are not envisioned or beyond the design basis of the system. Under-frequency load shedding is a notable example of this type of control. It operates when the system is in distress, and the resulting action of this control serves to help bring the system back into equilibrium. This design is elegant in that it is always appropriate to shed load when the system is experiencing a prolonged low frequency condition and that these controls can be autonomous and isolated, making them very secure and robust. Therefore, the presence of this type of control helps to enhance resilience, independent of the specific scenario or sequence of events that led up to its activation. Future implementation of under-frequency load shedding schemes will need to take into account the number of DERs on distribution feeders. These schemes may need to rely on intelligent load shedding instead of disconnecting entire distribution feeders.

### Intelligent Load Shedding

Automatic under-frequency load shedding is a common strategy designed into systems, which maintains the stability of the grid when there is an unanticipated loss of generation. Load shedding events typically impact entire circuits, with all customers on the circuit losing power (NERC, 2015). However, with increasing deployment of advanced metering infrastructure (AMI) and sectionalizing switches on distribution systems, opportunities exist to significantly improve the precision and reduce unwanted outages associated with load shedding events. In the near future, it may be possible for utilities to disconnect specific meters on a distribution circuit as opposed to disconnecting the entire circuit at the substation. Some AMI provide greater granularity in control, allowing fractional supply as opposed to only full or no supply. Load shedding could be made even more selective with

the installation of “smart” circuit breakers within customer facilities that would disconnect specific circuits within a residence or facility, based on providing appropriate financial incentives to customers. This could be done automatically, as a function of parameters like frequency, or it could be done under a systems optimization controller, but these different levels of functionality have differing levels of communication requirements.

**Recommendation 4.5:** The Department of Energy, working with the utility industry, should develop use cases and perform research on strategies for intelligent load shedding based on advanced metering infrastructure and customer technologies like smart circuit breakers. These strategies should be supported by appropriate system studies, laboratory testing with local measurements, and field trials to demonstrate efficacy.

### Adaptive Islanding

The process of “islanding” the grid—that is, where the interconnection breaks up or separates into smaller, potentially asynchronous portions—can result in significant outages if the islanding is the result of an uncontrolled cascading failure. However, there are opportunities to pre-plan and manage the islanding process such that outages impact significantly fewer customers. Adaptive islanding can preserve the benefits of large-scale interconnected system operations during normal conditions while reducing the risk of failures propagating across the grid during abnormal or emergency conditions.

Under normal system conditions, the track record of system protection is excellent. But performance during off-normal conditions is less predictable. When a cascading failure progresses through a power system, the individual tripping of transmission lines will often result in the formation of islands. The stability of an island post-disturbance depends predominantly on the balance of generation and load within the area and the ability to maintain that balance during the sequence of events leading up to, during, and after island formation. Generator protection might act to trip unit(s) to prevent damaging transients. The nature of these transients and their severity, and the ability of the remaining generation to match the load within the island, will determine whether the island will be stable. Other emergency controls, such as automatic under-frequency load shedding, are useful to help preserve the stability of an island as it is being formed. The goal of under-frequency load shedding is preventing the loss of generation from under-speed protection. Losing generation due to over-speed protection is less consequential because high frequency is the result of too much generation in the first place. Usually, one good indicator of whether an island will survive or fail is whether that region of the system was a net exporter or a net importer of power prior to the disturbance. It is easier for generation to throttle down than to

throttle up, although under-frequency load shedding schemes can also be used to maintain stability within the island.

Wide-area protection schemes have been developed to limit the consequences of an uncontrolled cascading failure (NERC, 2013). These remedial action schemes provide fast-acting control to preserve system stability in response to predefined contingencies. One such scheme deliberately separates the western power system into two islands by remotely disconnecting lines in the eastern portion of the system if key transmission paths in the western portion of the system become de-energized.

Adaptive islanding is an idea that has been under development for several years (You et al., 2004). The concept is predefining how to break apart the system in response to system events, by matching clusters of load and generation. The goal is to reduce the size of power system blackouts, and minimizing generation loss is a key element of this strategy. This can be accomplished through more aggressive use of fast-acting demand response to preserve the generation-load balance in each of the islands. The technology has progressed to the point where this is becoming a viable approach.

**Finding:** The electricity system, and associated supporting infrastructure, is susceptible to widespread uncontrolled cascading failure, based on the interconnected and interdependent nature of the networks.

**Recommendation 4.6:** The Department of Energy should initiate and support ongoing research programs to develop and demonstrate techniques for degraded operation of electricity infrastructure, including supporting infrastructure and cyber monitoring and control systems, where key subsystems are designed and operated to sustain critical functionality. This includes fault-tolerant control system architectures, cyber resilience approaches, distribution system interface with distributed energy resources, supply chain survivability, intelligent load shedding, and adaptive islanding schemes.

### Vulnerability Due to Interdependent Infrastructures

A reliable electric grid is crucial to modern society in part because it is crucial to so many other critical infrastructures, as described in Chapter 2. However, the dependency goes both ways, as the reliable operation of the grid depends on the performance of multiple supporting infrastructures. Outages can be caused by disruptions to natural gas production and delivery, commercial communications infrastructure, and transportation systems, among other critical infrastructures (Figure 4.5) (Rinaldi et al., 2001).

### Natural Gas Infrastructure

As described in Chapter 2, the fraction of generation provided by natural gas—both large central generating plants and small customer-owned generators powered by

internal combustion motors or microturbines—has grown substantially over the past few years. This not only exposes the industry to potential price volatility and supply chain vulnerability, but also raises the question of how utilities could restore electricity service if a major disruption to natural gas delivery occurred (e.g., one or more critical pipelines are destroyed). To date, no such outage has resulted in large electricity outages, and the minor events that have occurred fall on the scale of reliability operations that were handled relatively easily by the industry. The January 2014 Polar Vortex and the natural gas leak and subsequent closing of Aliso Canyon natural gas storage facility have already impacted utility planning and system design to be more cognizant of this critical interdependency (Box 4.2). These studies suggest that resilience can be enhanced through a diverse fuel portfolio, where a single interruption is less likely to impact a significant number of generators that cannot be overcome by reserve assets.

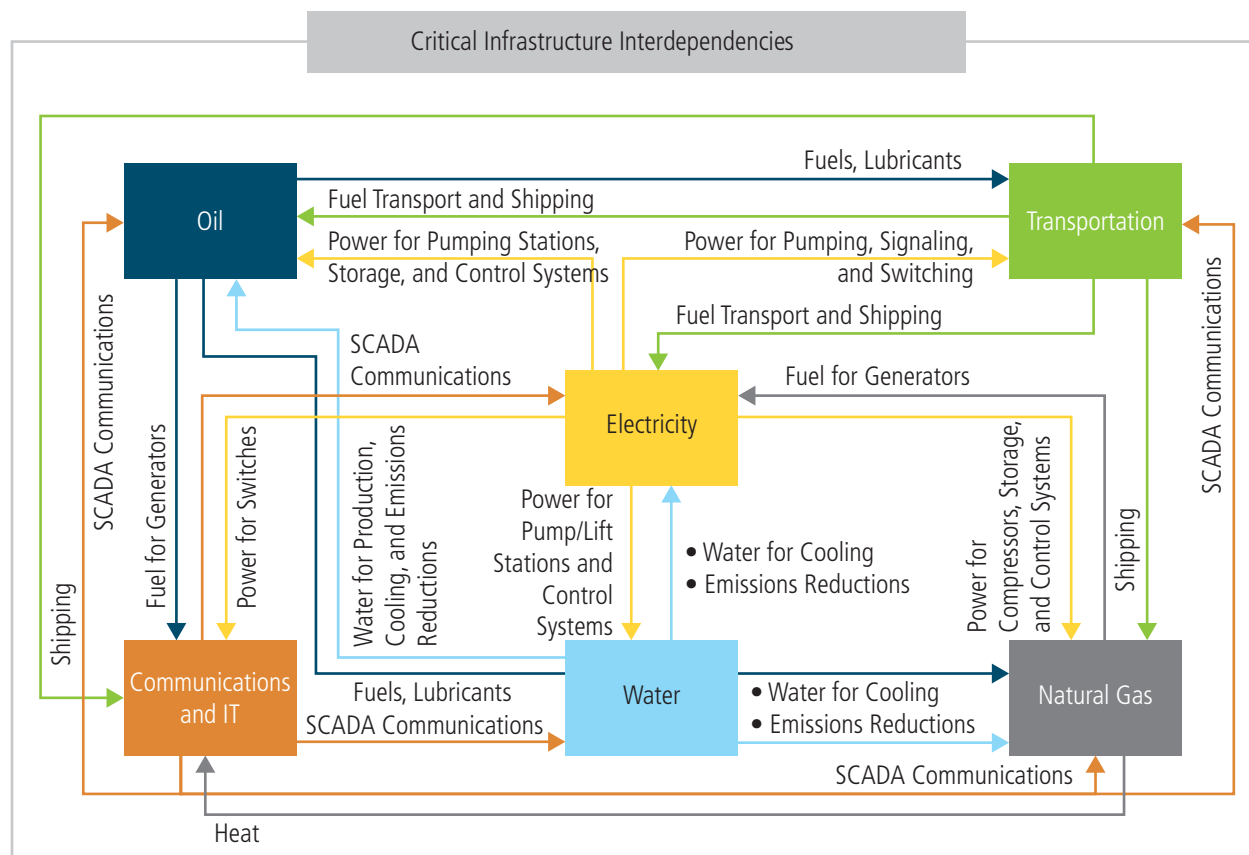
**Finding:** Constraints in natural gas infrastructure have resulted in shedding of electric load, and the growing interdependency of the two systems poses a vulnerability that could lead to a large-area, long-duration blackout.

**Recommendation 4.7:** The Federal Energy Regulatory Commission and the North American Energy Standards Board, in conjunction with industry stakeholders, should further prioritize their efforts to improve awareness, communications, coordination, and planning between the natural gas and electric industries. Such efforts should be extended to consider explicitly what recovery strategies should be employed in the case of failed interdependent infrastructure. Fuel diversity, dual fuel capability, and local storage should be explicitly addressed as part of these resilience strategies.

### Commercial Communications Infrastructure

Another example of coupled infrastructure is telecommunications. While many utilities utilize their own dedicated telecommunication assets to support critical communication and automation functions, there is a substantial dependency on communications and internet-based technologies that facilitate the daily operation of the modern electricity system, including coordination among personnel, managing markets, and financial structures, as well as supporting automation and control technology. With growing deployment of smart grid technologies and automated controls, this dependency may continue to increase. In the event of loss of external communications networks, many utility operations may be compromised, requiring greater reliance on manual operation and assessment of the state of damage. As an example, with the failure of multiple communications systems, it may be difficult to coordinate the activities of repair crews in the field with operational decisions, thus attenuating the hazards for workers and slowing the restoration.





**FIGURE 4.5** Disruption of any material or service that the electricity system relies on can result in loss of electric service and make restoration more challenging.

NOTE: SCADA, supervisory control and data acquisition.

SOURCE: DOE (2017).

### Design for Cyber Resilience

The electric power system has become increasingly reliant on its cyber infrastructure, including computers, communication networks, other control system electronics, smart meters, and other distribution-side cyber assets, in order to achieve its purpose of delivering electricity to the consumer. A compromise of the power grid control system or other portions of the grid cyber infrastructure itself can have serious consequences ranging from a simple disruption of service to permanent damage to hardware that can have long-lasting effects on the performance of the system. Any consideration of improved power grid resilience requires a consideration of improving the resilience of the grid's cyber infrastructure.

Over the past decade, much attention has rightly been placed on grid cybersecurity, but much less has been placed on grid cyber resilience. In particular, there has been significant research and investment in technologies and practices to prevent cyber attacks. Some of the many methods include the following: (1) identifying and apprehending cyber criminals, (2) defending the perimeter of a network with firewalls and

“white listing” and “black listing” certain communications sources, (3) practicing good cyber “hygiene” (e.g., protecting passwords and using two-factor authentication), (4) searching for and removing suspect pernicious code continuously, and (5) designing control systems with safer architecture—for example, segmenting systems to slow or prevent the spread of malware. The sources of guidance on protection as a mechanism to achieve grid cybersecurity are numerous (DOE, 2015); one good source of reference materials specific to industrial control systems can be found at the Department of Homeland Security’s Industrial Control System Cyber Emergency Response Team website.<sup>7</sup> Another good source of information is the Energy Sector Control Systems Working Group’s *Roadmap to Achieve Energy Delivery Systems Cyber Security* (ESCSWG, 2011). Furthermore, strategies to achieve power grid cybersecurity are documented in the National Institute for Standards and Technology Internal/

<sup>7</sup> The website for the Industrial Control System Cyber Emergency Response Team is <https://ics-cert.us-cert.gov/Standards-and-References>, accessed July 4, 2017.



Interagency Report 7628 *Guidelines for Smart Grid Cyber Security* (NISTIR, 2010). A good source of basic information is *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST, 2013), which, although nominally applying to federal information technology systems, has some guidance that can be useful in protecting grid cyber infrastructure.

It is now, however, becoming apparent that protection alone as a mechanism to achieve cybersecurity is insufficient and can never be made perfect. Cyber criminals are difficult to apprehend, and there are nearly 81,000 vulnerabilities in the National Institute of Standards and Technology (NIST) National Vulnerability Database, making it challenging to use safe code (NVD, 2016). An experiment conducted by the National Rural Electric Cooperative Association and N-Dimension in April 2014 determined that a typical small utility is probed or attacked every 3 seconds around the clock. Given the relentless attacks and the challenges of prevention, successful cyber penetrations are inevitable, and there is evidence of increases in the rate of penetration in the past year, particularly ransomware attacks.

Fortunately, the successful attacks to date have largely been concentrated on utility business systems as opposed to monitoring and control systems (termed operational technology [OT] systems), in part because there are fewer attack surfaces, fewer users with more limited privileges, greater use of encryption, and more use of analog technology. However, there is a substantial and growing risk of a successful breach of OT systems, and the potential impacts of such a breach could be significant. Serious risks are posed by further integration of OT systems with utility business systems, despite the potential for significant value and increased efficiency. Furthermore, the lure of the power of Internet protocols and cloud-based services threatens some of the practices that have historically protected the grid. Cloud-based services provide the potential for better reliability, resilience, and security versus on-premises computing, particularly for smaller utilities. For example, major commercial clouds, like the Amazon cloud, have a very high level of around-the-clock monitoring by a well-provisioned security operations center, better than that operated by some utilities. The cloud does, however, present another attack surface. Utilities that choose to use the cloud must explicitly consider the security of the cloud and how to secure the communications bi-directionally.

Given that protection cannot be made perfect, and the risk is growing, cyber resilience, in addition to more classical cyber protection approaches, is critically important. Cyber resilience aims to protect, using established cybersecurity techniques, the best one can but acknowledges that that protection can never be perfect and requires monitoring, detection, and response to provide continuous delivery of electrical service. While some work done under the cybersecurity nomenclature can support cyber resilience (e.g., intrusion detection and response), the majority of the work to date has been focused on preventing the occurrence of

successful attacks, rather than detecting and responding to partially successful attacks that occur.

Cyber resilience has a strong operational component (mechanisms must be provided to monitor, detect, and respond to attacks that occur), but it also has important design-time considerations. In particular, architectures that are resilient to cyber attacks are needed to support cyber resilience. Work during the past decade has resulted in “cybersecurity architectures” for the power grid cyber infrastructure, such as those described by NIST (2015), but there has been much less work done to define “cyber resilience architectures.” Some preliminary discussion of such an architecture can be found in MITRE’s *Cyber Resiliency Engineering Framework* (Bodeau and Graubart, 2011) and in NIST’s *Guidelines for Smart Grid Cyber Security* (NISTIR, 2010), among other places.

Generally speaking, a cyber resilience architecture should implement a strategy for tolerating cyber attacks and other impairments by monitoring the system and dynamically responding to perceived impairments to achieve resilience goals. The resilience goals for the cyber infrastructure require a clear understanding of the interaction between the cyber and physical portions of the power grid as well as how impairments on either (cyber or physical) side could impact the other side. By their nature, such goals are inherently system-specific but should balance the desire to minimize the amount of time a system is compromised and maximize the services provided by the system. Often, instead of taking the system off-line once an attack is detected, a cyber resilience architecture attempts to heal the system while providing critical cyber and physical services. Based on the resilience goals, cyber resilience architectures typically employ sensors to monitor the state of the system on all levels of abstraction. The data from multiple levels are then fused to create higher-level views of the system. Those views aid in detecting attacks and other cyber and physical impairments, as well as in identifying failure to deliver critical services. A response engine, often with human input, determines the best course of action. The goal, after perhaps multiple responses, is complete recovery (i.e., restoring the cyber system to a fully operational state).

Further work to define such cyber resilience architectures that protect, detect, respond, and recover from cyber attacks that occur is critically needed. Equally important, but just as challenging, is work to validate that proposed cyber resilience architectures achieve cyber resilience and cybersecurity requirements (see Recommendation 4.10).

### Regulatory and Institutional Opportunities

As described in Chapter 2, utilities seek and regularly receive regulatory approval for routine preventative maintenance activities such as vegetation management and hardening investments. While FERC regulates generation and interstate transmission, individual states are responsible

**BOX 4.3****Select Regulatory Actions Supporting Hardening, Modernization, and Other Preventative Investments****Florida Storm Hardening**

Given the recurring high risk of hurricane damage to electricity infrastructure in Florida, state regulators have long considered how to improve reliability and resilience to large storms. In a series of rulemakings in the mid-2000s, the Public Service Commission required that investor-owned utilities provide annual hurricane preparedness briefings, file and update storm hardening plans, increase coordination with local governments, and invest in research with Florida universities to improve robustness and recovery.

**Energy Strong New Jersey**

Following Superstorm Sandy and the extensive damage done to regional distribution systems and substations, the New Jersey Board of Public Utilities approved more than \$1 billion for hardening and modernizing Public Service Enterprise Group (PSEG) electric and gas infrastructure. Approximately \$600 million of this will go to elevating 29 substations damaged during Sandy to 1–2 feet above Federal Emergency Management Agency flood levels. An additional \$125 million will be used to install more sectionalizing switches in the distribution network, allowing PSEG to reconfigure the distribution systems and maintain service to the maximum number of customers during outage events.

**Connecticut Act Enhancing Emergency Preparedness and Response**

Passed following Hurricane Irene and major winter storms in 2011, this Act requires utilities to file emergency preparedness plans every 2 years with the state regulatory commission. Additionally, the Act provided grant funding for construction of microgrid projects at critical facilities around the state, and to date more than \$30 million has been invested in nearly 20 projects.

**Illinois Energy Infrastructure Modernization Act**

Passed by the state legislature in 2012, the Act authorizes Commonwealth Edison and Ameren Illinois to invest \$2.6 billion and \$625 million, respectively, in hardening, undergrounding, distribution automation, AML installations, and substation upgrades. The Act sets performance-based rates of return for utilities.

for approving investments in local transmission and the distribution system. There is wide variety in public utility commission (PUC) approval of utility investment across the United States and between geographically similar Gulf states (Carey, 2014). States along the hurricane-prone southeastern coast are more likely to allow alternative mechanisms to finance such investments, including the addition of “riders” to customer bills, securitization and issuance of bonds, and creation of reserve accounts that utilities can use as a form of self-insurance (EEI, 2014).

In addition to approving investments in hardening and preventative strategies, several states, such as California, Florida, and Connecticut, require utilities to regularly submit and update emergency preparedness plans, which often require input and coordination from city and county officials. Others provide performance-based incentives or penalties—for example, based on improvements to reliability measures such as SAIDI and SAIFI (although most reporting standards do not include large-area, long-duration outages when calculating these metrics)—to encourage best practices in the absence of standards on distribution systems. Other states impose penalties for inadequate levels of service or performance during storm events and recovery. Funding of grid modernization investments likewise varies across

states, with some regulator commissions such as California and Massachusetts researching and investing significantly in advanced communications and automation technologies. In the absence of regulatory approval, there is a critical opportunity for continuing federal grants (e.g., the Smart Grid Investment Grant provided to Chattanooga Electric Power Board) to further demonstrate the viability of such technologies and promote wider adoption across states.

In response to large outages such as those that resulted from Superstorm Sandy and other high-profile storms, state PUCs and, to a lesser extent, state legislatures across the country have considered investments in system hardening and implementing assorted grid modernization strategies with the goal of preventing or mitigating the impact of future large outages (Box 4.3).<sup>8</sup> Historically, such crises often provide the opportunity to focus attention and resources on costly robustness and resilience enhancements in a system that may be optimized economically without systematic consideration of the value of avoiding or responding quickly to these extreme events. Nonetheless, regulators’ and the industry’s efforts are more often reactive than proactive,

<sup>8</sup> A more complete review of state regulatory actions related to robustness and resilience is provided by EEI (2014).

and a focus on near-term cost-benefit optimization may not have resulted in investments that provide cost-effective benefits from a more resilient power grid. Thus, the committee expects that successfully funding cost-effective investments in resilience will require novel approaches, as described in Chapter 7, and proper metrics, as described in Recommendation 2.1.

## OPERATIONS

Much can be done in the area of real-time electric grid operations to enhance physical and cyber resilience. With the advent of smart grid devices, the electric grid is getting more intelligent with more sensing and embedded controls. While they are certainly beneficial, smart grid devices make the grid more complex. While this automatic control is helpful, any consideration of power system operations needs to recognize that the human operators are still very much “in the loop” and will continue to be so for many years into the future. Therefore, strategies to enhance operational resilience need to include tools to enhance the capabilities of the operators and engineers running the system.

In order to understand operations, it is useful to consider the different power system operating states shown in Figure 4.6. By far the majority of the time is spent in the normal state—that is, ready to handle the N-1 reliability criteria. This is the state in which people have the most experience; hence, many of the tools used in the control center are focused on normal operations. More rarely, the system moves into alert, emergency, and restorative situations. However, such situations are encountered often enough that there is good historical experience; control room personnel train for such situations, and, for the most part, they have adequate tools for dealing with these situations.

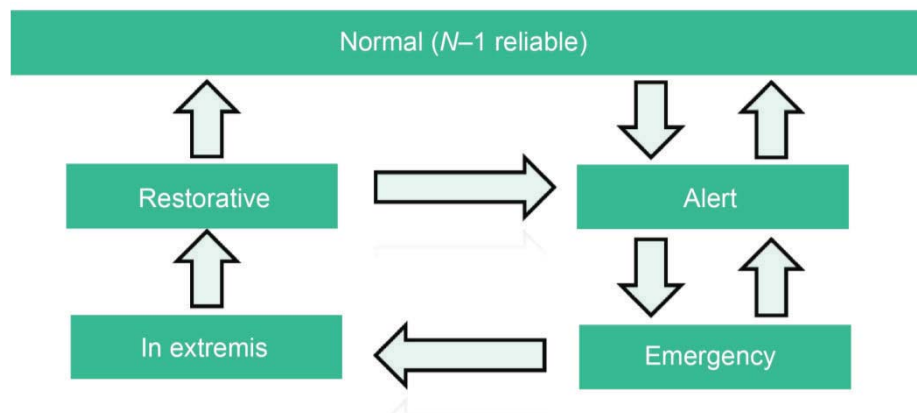
Enhancing grid resilience requires that more attention be given to the alert, emergency, in extremis, and restorative

stages of these operating states. In these stages, the previously interconnected grid may be broken into a number of electrical islands, and the operation of these islands may need to be performed by entities that are not normally responsible for grid operations (NERC, 2012a).

Sometimes, threats such as hurricanes can be identified with sufficient warning time to allow system operators to preemptively position the system to be more robust and able to respond to emerging conditions. This often involves curtailing any avoidable outages that might be caused by maintenance or other activities, deploying additional reserves to the extent possible, and even powering down certain critical components to minimize potential damage. This strategy is often less expensive than hardening strategies previously discussed. All major events are managed by operators in the control center, and their skills and training, as well as their tools and supporting technologies, are critical factors for how effectively the event will be managed.

## Wide-Area Monitoring and Control

As the power grid becomes more complex and is operated closer to reliability limits, the need for greater remote control increases. Fortunately, the technologies needed for such “wide-area control,” principally sensors and communications, are becoming cheaper and more powerful. The increasing use of high-speed wide-area measurements, including synchrophasors that measure currents and voltages 30–60 times a second and communicate them to distant computers, allows the design of controls that can use input data from different parts of the system and send control signals to equipment in different locations. The combination of PMUs, distribution automation, dedicated fiber-optic cable communications infrastructure, and affordable computing will likely lead to increasing reliance on artificial intelligence



**FIGURE 4.6** Power system operating states.

SOURCE: © 1978 IEEE. Reprinted, with permission, from *IEEE Spectrum Operating under Stress and Strain [electrical power systems control under emergency conditions]*.

in the power system. Additionally, remedial action schemes<sup>9</sup> are increasingly being deployed to increase the throughput of the grid, while minimizing the risk of cascading failures, by appropriately tripping loads and generators after an event on the system. The measurements for these automatic relays can often be hundreds of miles apart. These automated systems are able to sense and take action in real time, and can be thought of as a stepping stone to wider application of artificial intelligence and machine learning applied to the power grid.

Although such wide-area controls are appearing all over the world, the design, simulation, on-line testing, and cyber protection of such controls are expensive and time-consuming. Moreover, the architecture of the power grid and its overlaid control system has a direct impact on the design of such controls. For example, how centralized or decentralized a control scheme should be is constrained by where the measurements are, the communication paths to gather these measurements in the controller, and which equipment are available to this controller for control. Such controllers are in their evolutionary stages, so they should be designed not just for economic and reliability benefits, but also for resilience.

Often the term smart grid is used in reference to electronic meters and sensors. However, it also encompasses the wide-area monitoring and control considered here. That is, smart grids could include automatic sectionalizing, smart islanding to prevent cascading failures, the ability to operate these islands in a degraded state, and supercomputing resources to support system operators. For example, during the August 14, 2003, blackout, there was almost an hour of opportunity to intervene before the cascading event initiated (USCPSOTF, 2004). With better operational intelligence, a preventative shedding of approximately 2,000 MW load in the Cleveland area would have prevented the cascading failure that affected more than 60 million people.

During a major event such as Hurricane Katrina or Superstorm Sandy, thousands of alarms can overwhelm the system operator. Artificial intelligence could help quickly prioritize these alarms that come in over the supervisory control and data acquisition (SCADA)/energy management systems (EMS) and provide the operator with suggestions for the most important alarms to focus on, the root cause(s) of the event, and the most important actions to prevent further degradation and start restoration. The inherent complexity that power system operators have to face every day used to be addressed through detailed procedures. Today, with the system growing in complexity, the assistance of artificial intelligence and improved man-machine interfaces for system operators is likely to enhance both reliability and resilience. Under this scenario, all historical events and previous operators' experiences could be accumulated by a

system such as IBM's Watson to prioritize alarms and suggest appropriate action.

As DERs and smart inverters become more and more common in the distribution system, electricity system operators need to assess whether artificial intelligence combined with closed-loop fiber-optic broadband communication can improve the reliability and resilience for distribution customers. As more DERs are connected with smart inverters, the distribution system can break into smaller microgrids that can island and maintain service to critical load. In addition to distributed generation, demand side resources (customer loads) with inverters and power electronics can improve both reliability and resilience.

The Chattanooga EPB has demonstrated this by installing fiber-optic communication and automatic sectionalizing switches. Its communication system brought fiber optics to every home with smart meters available to determine both billing information and operational data such as Volts, Volt-ampere reactives, and Amps. This alone will not improve resilience, but combined with automated switches and voltage control devices EPB has greatly improved both the reliability and the resilience of its distribution system.

**Finding:** New automation systems promise to enable better monitoring and control of the grid. The design of such large-scale, wide-area controllers should be done with cyber resilience in mind. Such controllers should tolerate accidental failures and malicious attacks that occur, providing degraded functionality even during recovery from such attacks, and not be a hindrance during catastrophic events or the recovery afterwards. Flexibility of the controller may be achieved with the proper centralized/decentralized design, where the centralized control may provide the best benefits during normal operation. When the grid is broken up after a catastrophic event, however, the decentralized portion may still be able to operate the various parts.

### Physical and Cyber Situation Awareness

Bulk electric grids are some of the world's largest and most complex machines, and disturbances (cyber or physical) can rapidly propagate through their systems. Hence, normal operations can quickly change, demanding quick responses by the human operators or preprogrammed automation. Resilient operation requires physical and cyber "situation awareness," defined as "the perception of critical elements in the environment, the comprehension of their meaning, and the projection of their status into the future" (Wickens et al., 2013), so that unfavorable changes of physical or cyber state that occur can be addressed (either by human or automated means) quickly enough to prevent a catastrophic event.

In the power industry, the term "situation awareness" was popularized by the August 14, 2003, *Blackout Final Report* in which "inadequate situational awareness at First Energy"

<sup>9</sup> A scheme designed to detect predetermined system conditions and automatically take corrective actions that may include, but are not limited to, adjusting or tripping generation, tripping load, or reconfiguring a system (NERC, 2014c).



was noted as the second of the four root causes of the event (USCPSOTF, 2004). The importance of system understanding was also highlighted in the first and fourth causes of the event: “FirstEnergy (FE) and ECAR (East Central Area Reliability Council) failed to assess and understand the inadequacies of First Energy’s system, particularly with respect to voltage instability and the vulnerability of the Cleveland-Akron area, and FE did not operate its system with appropriate voltage criteria. . . . [T]he interconnected grid’s reliability organizations [failed] to provide effective real-time diagnostic support” (USCPSOTF, 2004). If operators were aware of the accurate estimate of the “true state” of the grid, they could have taken appropriate actions, which would have eliminated the propagation of effects that led to the widespread blackout. Thus real-time determination of the combined physical and cyber state of the grid is needed to achieve resilience.

Whether operator action can prevent a blackout depends on the time frame and severity of the event (Overbye and Weber, 2015). Some large-scale blackouts cannot be prevented by operator action; earthquakes are examples of unanticipated events that can cause severe damage within seconds. Cyber attacks also have the potential to spread extremely quickly. Conversely, slow-moving weather systems such as hurricanes or ice storms give operators plenty of time to act, but the blackouts cannot be fully prevented. As an example, an ice storm in January 1998 resulted in the collapse of more than 770 transmission towers, causing a large-scale blackout in Canada (Hauer and Dagle, 1999), and Superstorm Sandy caused 8.5 million customer power outages in 2012 (Abi-Samra et al., 2014). The same might be true of the pandemics that would severely limit human resources for response (NERC, 2010).

However, many potential blackouts, including a number of the severe events considered here, do have time frames that could allow for effective operator intervention. North American examples include the August 14, 2003, blackout that affected more than 50 million people, in which more than an hour passed between the system being outside of the normal secure state (remaining stable following the next contingency) and the final uncontrolled cascading failure leading to the blackout (USCPSOTF, 2004); and the September 8, 2011, Western Electricity Coordinating Council blackout that had an 11-minute period between the initiating event and the blackout, and that cited lack of situation awareness as a cause (FERC and NERC, 2012). A primary reason for these time frames is the underlying power system dynamics, including the time constants associated with thermal heating on transmission lines and transformers, the operation of load-tap-changing transformers, protective relaying time constants, and other system limits. Another reason would be the dynamics associated with the initiating event; for a GMD, this might be minutes to hours. Having good power system situation awareness, even during periods of extremely unusual system stress, is crucial for enhancing overall grid resilience.

Furthermore, propagation of disturbances through the grid can potentially be mitigated before a catastrophic event occurs though the use of cyber-resilient, computer-enabled, automated monitoring and state estimation, diagnosis, response, and recovery. While humans can only react on time scales that are in seconds-to-minutes, computer-enabled diagnosis, response, and recovery can operate on the time scale of microseconds-to-seconds, effectively halting the propagation of adverse effects before they progress to a stage where they can no longer be mitigated. Hence the development of (1) deep and diverse monitoring mechanisms, (2) computerized monitor data fusion methods, and (3) computerized response selection and actuation methods that themselves are cyber resilient is essential to providing resilience in the face of a wide variety of impairments.

### Cyber-Resilient Monitoring of Physical and Cyber States

Regarding monitoring, methods must be developed to determine the amount and diversity of monitoring necessary to gain the cyber and physical situation awareness to effectively respond to particular classes of impairments. Today, monitor selection and deployment is typically a static and off-line process. Methods are also needed to increase the confidence in the monitoring data that are obtained. It is critical that the state estimated from the monitoring data used by a resilience strategy is not influenced by bad data (created either inadvertently or through deliberate attacker action) so as to avoid response decisions that compromise resilience.

### Monitor Data Fusion

A key challenge with the effective use of monitor data (whether cyber or physical) is their volume. In order to make sense of this large volume of monitor data, methods are needed to fuse the data into higher level knowledge about the state of the grid, creating actionable situation awareness. Fusion, in this context, is defined as the process to combine information from multiple sources to achieve inferences, which will be more efficient and more accurate than if they were achieved through a single source. A key challenge in the power grid context is that monitoring data concerning both the physical and cyber state of the grid is needed and must be fused together to understand the state of the system to the degree that response actions to preserve correct operation can be taken.

Understanding of the system is complicated by the fact that when a monitor signals a problem, it is unclear whether the problem is with the component or sub-system that is being monitored or with the monitor itself (particularly if malicious actions might cause erroneous monitor data). Monitoring of the state of both cyber and physical aspects of the grid is essential and must be sufficiently powerful to diagnose whether the error-condition being observed is due to a cyber and/or physical impairment. While it has been long



understood that the monitoring of physical aspects of the grid is needed, the criticality of the monitoring of the state of the grid's cyber components is less understood.

Human operators will continue to play a key role in grid operations for decades to come, and they can certainly help in the fusion of information. Important goals include minimizing the overhead on human experts and learning from the monitor data to identify important features that can contribute to lack of resilience. It would also be valuable if these techniques are computationally lightweight. This would allow operators to incorporate these techniques in the system to work online.

### Response Selection and Actuation

Timely response to detection of undesirable state conditions is critical to maintain the grid's ability to deliver power despite impairments that occur. In order to be effective, determination of response actions must be efficient and scalable. In particular, a resilience response mechanism must respond quickly in a way that limits the cyber or

physical impairment (whether accidental or intentional) from propagating to the point that a catastrophic event occurs. Furthermore, resilience response mechanisms must be scalable, in order to account for the unique physical and cyber complexity of the grid and the large volume of monitor data that must be collected, to obtain an accurate estimate of the state of the system.

During the unusual situations associated with severe events, wide-area power system visualization is crucial for providing the operators and engineers with the "big picture" of a grid that may be operating in a physical and/or cyber state they have not previously encountered. There may be multiple electric islands, transmission line flows may be substantially different from normal, and the voltage profile could be quite unusual. Often this wide-area view is provided in a control center using a mapboard, such as the one used by Independent System Operator (ISO) New England's control center, shown in Figure 4.7. As noted by Overbye and Weber (2015), such wide-area visualizations are divided into two main types. The first approach is to draw the display using fairly precise geographic coordinates. An example of this



**FIGURE 4.7** ISO New England control room.  
SOURCE: ISONE (2013).

is shown for the synthetic network in Figure 4.4 or in the coupling with the earthquake simulations by Veeramany et al. (2016). Advantages include the ability to overlay power system information with other infrastructures and a familiar context when communicating with non-power engineers. A key disadvantage is that often the locations with a large amount of electrical infrastructure, such as urban areas, have a small geographic footprint. An alternative approach is to use a pseudo-geographic layout in which the position of the power system elements has some relationship with their actual geographic coordinates, but the display is arranged for electrical clarity. This approach was used in the ISO New England control center, which, while covering all of New England, has much of the display devoted to the greater Boston area. Additional visualization techniques, such as color contouring, focus on displaying large amounts of power system information (Weber and Overbye, 2000).

There is also a need to consider the human factors of severe events in the control room context. During such events, there would certainly be a high level of stress, and, while expert operators would be better prepared than less experienced personnel, successful decisions are far from guaranteed. Wickens et al. (2013) explain, “Cues may be uncorrelated, overconfidence may shortchange cognitive monitoring, and rapid pattern-recognition classification may overlook a single outlying cause.” There may also be a “confirmation bias,” which “describes a tendency for people to seek information and cues that confirm the tentatively held hypothesis or seek (or discount) those that support an opposite conclusion or belief” (Wickens et al., 2013). This reinforces the importance of training and drills that provide operators with simulated experience.

**Finding:** Bulk electric grids are not only some of the world's largest and most complex machines, but they also have been architected in a way that disturbances can, if not mitigated, rapidly propagate through the system. Maintaining physical and cyber situation awareness at all times is key. Lack of situation awareness has been a contributing factor in a number of recent large-scale outages. During severe events, this will be even more of a challenge; therefore, there is a need for work on the development of data analytics and visualization techniques that will allow operators and engineers to maintain cyber and physical situation awareness.

**Recommendation 4.8:** The Department of Energy and the National Science Foundation should fund research on enhanced power system wide-area monitoring and control and on the application of artificial intelligence to the power system. Such work should include how the human-computer interface and visualization could improve reliability and resilience. In particular, the Department of Energy should develop research programs on enhancing power grid control room cyber and physical situation awareness with a focus on severe event situations.

### Monitoring of Grid Cyber System State to Achieve Physical and Cyber Resilience

The proper functioning of the grid's various cyber systems (e.g., computers, communications) directly affects the ability to monitor, operate, and control the power system, thus making it imperative that the cyber system itself also be resilient. Like the physical aspects of the power grid, these cyber systems can be affected by catastrophic events like storms and earthquakes and are directly vulnerable to cyber attacks. These supporting systems are often considered critical and are usually designed with enough redundancy to provide reliability to accidental faults. It is critical to have situation awareness of the state of information systems alongside operations systems, as detailed in the concept of an integrated security operations center (EPRI, 2013).

While existing NERC standards provide some requirements with respect to cybersecurity, no standards or widespread best practices exist for tolerating deliberate cyber attacks. Moreover, monitoring of the system itself has been less stringent than that of the power system, and, unlike the power system, the status of the control system is rarely shared with that of the neighboring power companies. For example, during the 2003 Northeast blackout the neighboring power companies were not aware that several of the monitoring functions like alarm processing and state estimation were not functioning at the Akron, Ohio, control center.

Even less common is the use of architectural approaches to ensure the resilience of the cyber system to accidental failures and malicious attacks. As noted, the operation of an interconnected power grid requires the cooperation of many entities, mostly done through the coordination among dozens of control centers. Thus, the health of the control and communications systems should also be continuously monitored by these control centers. These monitoring data should be used to take actions to maintain the resilience of the cyber system itself to both accidental failures and malicious attacks and be shared with all the others who depend on this coordination.

Unfortunately, data gathering and analysis are often performed separately and differently between neighboring utilities and between T&D sections within the same power company. More coordination between these jurisdictions would be helpful during normal operations; the lack of it severely affects the ability to prevent large-scale catastrophes like a cascading failure or cyber attack. During such an event that impacts several power companies, effective communication of data among utilities can help inform and accelerate decisions that may avoid permanent damage to existing hardware or prevent widespread outages. The main issue in coordinating these various functions has been the lack of standardization of data definitions, databases, and communication protocols. Moreover, data exchange between neighbors also raises some proprietary issues. However, if resilience is to be increased and the ability to recover from catastrophic events is to be accelerated, such coordination between T&D in the same

company and between interconnected neighboring companies is necessary. Although the utility industry has a long record of collaboration during large-scale disturbances, this is still done more on an ad hoc basis; the type of coordination suggested here must be planned, and the tools must be in place long before the catastrophe.

Achieving greater standardization is important and an active research area in Europe, providing opportunities for strong coordination (EDSO, 2015). However, as that occurs, it is important to devote serious attention to cybersecurity lest identical control equipment, with identical vulnerabilities, be used by multiple companies. This could make the system particularly vulnerable to a cyber attack that could be widespread and affect multiple utilities simultaneously.

**Finding:** The cyber system that monitors, analyzes, and controls the physical components of the power grid is critical to providing efficient and reliable service from the grid. Less attention has been placed on making these cyber systems resilient. Furthermore, the various control systems of an interconnected power grid fall under many different jurisdictions, and close coordination is needed for the design and operation so that information exchange in real time is seamless and timely and response actions are taken in a coordinated way.

**Finding:** Currently, there is a lack of standardized information sharing among utilities at the T&D levels. In some cases, such as cyber health data, the data requirements have not yet been defined. As greater standardization is achieved, greater attention must also be given to cybersecurity and risks of common-mode failures.

**Recommendation 4.9:** The Department of Energy should lead and coordinate an effort among the Federal Energy Regulatory Commission, the North American Electric Reliability Corporation, the National Association of Regulatory Utility Commissioners, and the states to develop standardized data definitions, communication protocols, and industrial control system designs for the sharing of both physical and cyber system health information. The goal of standardizing data definitions and communication protocols would be to improve the awareness of the operating conditions of all interconnected power systems for all involved transmission operators and distribution operators.

### Architectures for Providing Cyber and Physical Resilience

A wide range of cyber systems are used to protect and control the grid. In operations, the time requirements for response to maintain resilience range from a few milliseconds (e.g., for protective relays controlling circuit breakers that clear faults), to seconds (e.g., for the automatic generation control that provides real-time dispatch to generators), to several seconds to minutes (e.g., for the software used by

the operators for human-in-the-loop control). Much of this architecture, and its enhancement via synchrophasors, is discussed by Bose (2010).

Transmission operators use EMS to monitor and control the grid. Almost all of the real-time measurements input to the EMS come from SCADA systems, which scan the grid every 2 to 4 seconds. An important component of EMS is the monitoring/alarming system that notifies the operator when unusual situations are encountered. This alarm system failed for one transmission operator leading up to the August 14, 2003, blackout, which contributed to its lack of situation awareness (USCPSOTF, 2004). As the name implies, SCADA is used for direct monitoring and control of the grid. A failure of SCADA, such as from a cyber intrusion, would make operations very difficult, requiring personnel to be physically located at key electric substations. Over the past several years, the SCADA data are increasingly being supplemented by PMU data, which uses much faster scan rates of 30 to 60 times per second, allowing direct measurement of the voltage and current phase angles (NASPI, 2015).

In order to run more advanced grid analysis techniques in real time, the imperfect measurements from SCADA (and sometimes PMUs) are input to a process known as state estimation. State estimation is run every few minutes to obtain a best estimate of power system voltages and currents. The output of the state estimator is then fed to applications such as power flow, contingency analysis, security-constrained optimal power flow, and transient stability analysis. State estimation is a maximum likelihood estimator that uses iterative algorithms. In a modern control center, the state estimator might be solving on the order of 250,000 measurements every minute, with convergence rates well over 98 percent of the time (PJM, 2016). However, during unusual situations associated with severe events, convergence of the state estimator itself might be an issue. This was the case during the August 14, 2003, blackout, in which lack of convergence in the Midwest Independent Transmission System Operator state estimator contributed to its inability to provide real-time diagnostic support (USCPSOTF, 2004).

The grid was operated for more than half a century before computers were invented and can still be, in many cases, operated in a degraded way without the advantages of the computerized control system. In fact, the cyber attack on the Ukraine system forced the operators to operate the power grid with reduced levels of service without the automation system, which was badly compromised.

**Finding:** The control system for the power grid must be designed and operated in a way that allows it to tolerate both accidental faults and malicious attacks. Best practices from the dependable computing community and the emerging cyber resilience community could be employed and extended to make the grid cyber infrastructure itself resilient. Moreover, the interfaces between the cyber control system and the physical aspects of the power grid could be designed



in such a way that the power grid can be operated without automation, albeit in a degraded mode. This would require some control functions to be performed manually during catastrophic events, thus requiring personnel to be trained and ready to perform functions that would rarely be needed.

**Recommendation 4.10:** The Department of Energy should embark upon a research, development, and demonstration program, utilizing the diverse expertise of industry, academia, and national laboratories, that results in a prototypical cyber-physical-social control system architecture for resilient electric power systems. The program would have the following components: (1) A diverse set of sensors (spanning the physical, cyber, and social domains), (2) a method to fuse this sensor data together to provide situation awareness of known high quality, and (3) an ability to generate real-time command and control recommendations for adaptations that should be taken to maintain the resilience of an electric power system. This should include research to develop methods for specifying anomalous operating conditions, so that anomaly detection systems can be deployed widely to aid in the detection of cyber intrusions. In this process, the Department of Energy should coordinate with standards-setting organizations. Analytic arguments should be constructed so that these recommendations do not compromise the safety or availability of the system.

## REFERENCES

- Abi-Samra, N., J. McConnach, S. Mukhopadhyay, and B. Wojszczyk. 2014. When the bough breaks: Managing extreme weather events affecting electrical power grids. *IEEE Power and Energy Magazine* 12(5): 61–65.
- Albertson, V.D., J.M. Thorson Jr., R.E. Clayton, and S.C. Tripathy. 1973. Solar-induced currents in power systems: Cause and effects. *IEEE Transactions on Power Apparatus and Systems* PAS-92(2): 471–477.
- ARPA-E (Advanced Research Projects Agency-Energy). 2016. "Grid Data." <https://arpa-e.energy.gov/?q=arpa-e-programs/grid-data>. Accessed July 13, 2017.
- Bedrosian, P.A., and J.J. Love. 2015. Mapping geoelectric fields during magnetic storms: Synthetic analysis of empirical United States impedances. *Geophysical Research Letters* 42(10): 160–170.
- Birchfield, A.B., T. Xu, K. Gegner, K.S. Shetye, and T.J. Overbye. 2016. Grid structural characteristics as validation criteria for synthetic networks. *IEEE Transactions on Power Systems* 32(4): 3258–3265.
- Bodeau, D.J., and R. Graubart. 2011. *Cyber Resiliency Engineering Framework*. MITRE Technical Report 110237. [https://www.mitre.org/sites/default/files/pdf/11\\_4436.pdf](https://www.mitre.org/sites/default/files/pdf/11_4436.pdf).
- Bose, A. 2010. Smart transmission grid applications and their supporting infrastructure. *IEEE Transactions on Smart Grid* 1(1): 11–19.
- Boteler, D. 1994. Geomagnetically induced currents: Present knowledge and future research. *IEEE Transactions on Power Delivery* 9(1): 50–58.
- Carey, K. 2014. *The Day After Tomorrow: A Survey of How Gulf Coast State Utility Commissions and Utilities are Preparing for Future Storms*. <http://wordpress.ei.columbia.edu/climate-change-law/files/2016/06/Carey-2014-03-Gulf-Coast-State-Utility-Commissions-Storm-Preparation.pdf>.
- CEC (California Energy Commission). 2016. *Aliso Canyon Action Plan to Preserve Gas and Electric Reliability for the Los Angeles Basin*. [http://www.energy.ca.gov/2016\\_energypolicy/documents/2016-04-08\\_joint\\_agency\\_workshop/Aliso\\_Canyon\\_Action\\_Plan\\_to\\_Preserve\\_Gas\\_and\\_Electric\\_Reliability\\_for\\_the\\_Los\\_Angeles\\_Basin.pdf](http://www.energy.ca.gov/2016_energypolicy/documents/2016-04-08_joint_agency_workshop/Aliso_Canyon_Action_Plan_to_Preserve_Gas_and_Electric_Reliability_for_the_Los_Angeles_Basin.pdf).
- DOE (Department of Energy). 2011. *A Smarter Electric Circuit: Electric Power Board of Chattanooga Makes the Switch*. [https://www.smartgrid.gov/files/EPB\\_Profile\\_casestudy.pdf](https://www.smartgrid.gov/files/EPB_Profile_casestudy.pdf).
- DOE. 2015. *Energy Sector Cybersecurity Framework Implementation Guidance*. [https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance\\_FINAL\\_01-05-15.pdf](https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf).
- DOE. 2017. *Quadrennial Energy Review: Transforming the Nation's Electricity System: The Second Installment of the QER*. <https://energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review-Second%20Installment%20%28Full%20Report%29.pdf>.
- EDSO (European Distribution System Operators for Smart Grids). 2015. *Coordination of Transmission and Distribution System Operators: A Key Step of the Energy Union*. <http://www.edsoforsmartgrids.eu/wp-content/uploads/public/Coordination-of-transmission-and-distribution-system-operators-May-2015.pdf>.
- EEL (Edison Electric Institute). 2014. *Before and After the Storm*. <http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/BeforeandAftertheStorm.pdf>.
- EPRI (Electric Power Research Institute). 2013. *Guidelines for Planning an Integrated Security Operations Center*. EPRI Report # 3002000374. Palo Alto, Calif.: EPRI.
- ESCSWG (Energy Sector Control Systems Working Group). 2011. *Roadmap to Achieve Energy Delivery Systems Cyber Security*. [https://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap\\_finalweb.pdf](https://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf).
- FERC (Federal Energy Regulatory Commission) and NERC (North American Electric Reliability Corporation). 2012. *Arizona-Southern California Outages on September 8, 2011: Causes and Recommendations*. <https://www.ferc.gov/legal/staff-reports/04-27-2012-ferc-nerc-report.pdf>.
- Glass, J. 2016. "Enhancing the Resiliency of the Nation's Electric Power Transmission and Distribution System," presentation to the Committee on Enhancing the Resilience of the Nation's Electric Power Transmission and Distribution System, September 29, Washington, D.C.
- Hart, D., and A. Sarkissian. 2016. *Deployment of Grid-Scale Batteries in the United States*. <https://energy.gov/sites/prod/files/2017/01/f34/Deployment%20of%20Grid-Scale%20Batteries%20in%20the%20United%20States.pdf>.
- Hauer, J.F., and J.E. Dagle. 1999. *Consortium for Electric Reliability Technology Solutions: Grid of the Future*. PNNL-13150. Richland: Pacific Northwest National Laboratory.
- Hutchins, T., and T.J. Overbye. 2016. Power system dynamic performance during the late-time (E3) high-altitude electromagnetic pulse. *Proceedings of the 19th Power Systems Computation Conference*. Genoa, Italy, June 20–24.
- ICF. 2016. *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*. <https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf>.
- IEEE (Institute of Electrical and Electronics Engineers). 2017. "Project P1547—Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces." <https://standards.ieee.org/develop/project/1547.html>. Accessed March 2017.
- ISONE (Independent System Operator New England). 2013. ISO New England Control Room. <https://www.linkedin.com/company/iso-new-england>. Accessed July 11, 2017.
- Lordan, R. 2016. "Transmission Resiliency & Security Response to High Impact Low Frequency Threats," presentation at the NCSL-NARUC Energy Risk & Critical Infrastructure Protection Workshop, May 25, Denver, Colo.

- NASEM (National Academies of Sciences, Engineering, and Medicine). 2016a. *Electricity Use in Rural and Islanded Communities: Proceedings of a Workshop*. Washington, D.C.: The National Academies Press.
- NASEM. 2016b. *Analytic Research Foundations for the Next-Generation Electric Grid*. Washington, D.C.: The National Academies Press.
- NASPI (North American Synchrophasor Initiative). 2015. *NASPI 2014 Survey of Synchrophasor System Networks—Results and Findings*. <https://www.naspi.org/documents>. Accessed July 11, 2017.
- NERC (North American Electric Reliability Corporation). 2005. *TLP-001-4—Transmission System Planning Performance Requirements*. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=TPL-001-4&title=Transmission%20System%20Planning%20Performance%20Requirements&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-001-4&title=Transmission%20System%20Planning%20Performance%20Requirements&jurisdiction=United%20States). Accessed January 12, 2017.
- NERC. 2010. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*. <http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf>.
- NERC. 2011. *Report on Outages and Curtailments During the Southwest Cold Weather Event of February 1–5, 2011*. [http://www.nerc.com/files/sw\\_cold\\_weather\\_event\\_final\\_report.pdf](http://www.nerc.com/files/sw_cold_weather_event_final_report.pdf).
- NERC. 2012a. *Severe Impact Resilience: Considerations and Recommendations*. [http://www.nerc.com/docs/oc/sirtf/SIRTF\\_Final\\_May\\_9\\_2012-Board\\_Accepted.pdf](http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf).
- NERC. 2012b. *Special Reliability Assessment Interim Report: Effects of Geomagnetic Disturbances on the Bulk Power System*. <http://www.nerc.com/files/2012GMD.pdf>.
- NERC. 2013. *Protection System Response to Power Swings*. [http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report\\_Final\\_20131015.pdf](http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%2020/SPCS%20Power%20Swing%20Report_Final_20131015.pdf).
- NERC. 2014a. *Standard CIP-014-2*. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=PhysicalSecurity&jurisdiction=null](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-014-2&title=PhysicalSecurity&jurisdiction=null). Accessed January 12, 2017.
- NERC. 2014b. *Polar Vortex Review*. [http://www.nerc.com/pa/rtrm/January%202014%20Polar%20Vortex%20Review/Polar\\_Vortex\\_Review\\_29\\_Sept\\_2014\\_Final.pdf](http://www.nerc.com/pa/rtrm/January%202014%20Polar%20Vortex%20Review/Polar_Vortex_Review_29_Sept_2014_Final.pdf).
- NERC. 2014c. *Remedial Action Scheme: Definition Development*. [http://www.nerc.com/pa/Stand/Prjct201005\\_2SpclPrctnSstmPhs2/FAQ\\_RAS\\_Definition\\_0604\\_final.pdf](http://www.nerc.com/pa/Stand/Prjct201005_2SpclPrctnSstmPhs2/FAQ_RAS_Definition_0604_final.pdf).
- NERC. 2015. *PRC-006-2—Automatic Underfrequency Load Shedding*. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=PRC-006-2&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=PRC-006-2&title=Automatic%20Underfrequency%20Load%20Shedding&jurisdiction=United%20States). Accessed January 12, 2017.
- NERC. 2016a. *TPL-007-1—Transmission System Planned Performance for Geomagnetic Disturbance Events*. [http://www.nerc.com/\\_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States](http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=TPL-007-1&title=Transmission%20System%20Planned%20Performance%20for%20Geomagnetic%20Disturbance%20Events&jurisdiction=United%20States). Accessed July 3, 2017.
- NERC. 2016b. *Short-term Special Assessment*. [http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20GAS%20Electric\\_Final.pdf](http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20Short-Term%20Special%20Assessment%20GAS%20Electric_Final.pdf).
- NIST (National Institute of Standards and Technology). 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST Special Publication 800-53. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.
- NIST. 2015. *Guide to Industrial Control Systems (ICS) Cybersecurity*. NIST Special Publication 800-82. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>.
- NISTIR (National Institute of Standards and Technology Internal/Interagency Reports). 2010. *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*. [https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628\\_total.pdf](https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf).
- NREL (National Renewable Energy Laboratory). 2014. *Issue Brief: A Survey of State Policies to Support Utility-Scale and Distributed Energy Storage*. <http://www.nrel.gov/docs/fy14osti/62726.pdf>.
- NVD (National Vulnerability Database). 2016. National Vulnerability Database (NVD)—NVD Dashboard. <https://nvd.nist.gov/general/nvd-dashboard>. Accessed July 11, 2017.
- Overbye, T.J., and J.D. Weber. 2015. Smart grid wide-area transmission system visualization. *Engineering* 1(4): 466–474.
- Overbye, T.J., T.R. Hutchins, K. Shetye, J. Weber, and S. Dahman. 2012. Integration of geomagnetic disturbance modeling into the power flow: A methodology for large-scale system studies. *Proceedings of the 2012 North American Power Symposium*. Champaign, Ill., September 9–11.
- PJM. 2016. *Operations Support Division, Energy Management System (EMS) Model Updates and Quality Assurance (QA) Manual M-03A (Revision 12)*. <http://www.pjm.com/~media/documents/manuals/m03a.ashx>. Accessed July 11, 2017.
- Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly. 2001. Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine* 21(6): 11–25.
- Rivera, M., and M. Backhaus. 2015. *Review of the GMD Benchmark Event in TPL-007-1*. Los Alamos National Laboratory. [http://www.energy.gov/sites/prod/files/2015/09/f26/TPL-007-1%20Review\\_LANL\\_2015\\_09\\_14.pdf](http://www.energy.gov/sites/prod/files/2015/09/f26/TPL-007-1%20Review_LANL_2015_09_14.pdf).
- USCPSOTF (U.S.–Canada Power System Outage Task Force). 2004. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. <http://www.nerc.com/docs/docs/blackout/ch1-3.pdf>.
- Veeramany, A., G.A. Coles, S.D. Unwin, T.B. Nguyen, and J.E. Dagle. 2016. *Trial Implementation of the High-Impact, Low-Frequency Power Grid Event Risk Framework to Support Informed Decision-Making Placeholder on Earthquakes*. Richland, Wash.: Pacific Northwest National Laboratory.
- Wade, D. 2016. “Increasing the Resiliency/Reliability of the EPB System,” presentation at the Electricity Use in Rural and Islanded Communities: A Workshop Supporting the Quadrennial Energy Review’s Public Outreach, February 8, Washington, D.C.
- Weber, J.D., and T. J. Overbye. 2000. Voltage contours for power system visualization. *IEEE Trans. on Power Systems* 15(1): 404–409.
- Wickens, C.D., J.G. Hollands, S. Banbury, and R. Parasuraman. 2013. *Engineering Psychology and Human Performance*. Fourth Edition. Boston: Pearson.
- Wischkaemper, J.A., C.L. Benner, B.D. Russell, and K.M. Manivannan. 2014. “Waveform Analytics-based Improvements in Situational Awareness, Feeder, Visibility, and Operational Efficiency.” *Proceedings of the 2014 IEEE PES T&D Conference and Exposition*. doi:10.1109/tdc.2014.6863349.
- Wischkaemper, J.A., C.L. Benner, B.D. Russell, and K.M. Manivannan. 2015. Application of waveform analytics for improved situational awareness of electric distribution feeders. *IEEE Transactions on Smart Grid* 6(4): 2041–2049.
- You, H., V. Vittal, and X. Wang. 2004. Slow coherency-based islanding. *IEEE Transactions on Power Systems* 19(1): 483–491.



## 5

## Strategies for Reducing the Harmful Consequences from Loss of Grid Power

### INTRODUCTION

Chapter 4 examined planning, design, and operations that can help improve the reliability and resilience of the grid to prevent or reduce the duration of grid outages. Chapter 6 looks at restoration of grid service. But in the middle sits the question of how to design and plan for a society that will be resilient even with the loss of power. This chapter examines current and future responses to that question. As introduced in Chapter 3, the exact form of that planning depends on the causes of grid failure, because those causes may affect which other services are available and the speed and extent of restoration (see Figure 3.2). Full restoration, as explored in Chapter 6, may take a long time—during and after which the effects of lost grid service could continue to reverberate through society.

As in the other sections of this report, the committee does not focus much on small routine disruptions that are inherent to power distribution systems. Those outages, because they are short and familiar, do not create major resilience problems; their effects are usually local, understood, and well within the range of imagination and planning. Indeed, in a typical year there are about 3,200 significant outages on power grids in the United States, with extreme weather and falling trees as leading causes (Eaton, 2016). In a 2015 Harris poll, homeowners self-reported that one out of four had experienced power outages for 12 hours or longer in the past 2 years (Briggs and Stratton, 2015). These are common events that generate large costs to the economy and public welfare—for example, jeopardizing the continued operation of home health care equipment (Ryan et al., 2015) as well as continuity of important public functions and economic activity such as data centers (Vertiv, 2016)—but are within the realm of normal experience and planning.

Instead, the committee focuses on large regional disruptions that last for several days or longer and cover a larger area, such as multiple service territories or even several states. Such long duration outages do occur, as shown in Figure 1.1 and discussed later in this chapter. Such events,

which can have profound system-wide effects, require much more attention than they have received to date from policy makers and every segment of society that depends on electric service. Because these effects are outside the realm of normal experience, it is difficult for people and organizations to imagine the possible harmful outcomes on the basis of real-world information about consequences. Reducing these harmful consequences of large-area, long-duration grid failures is a problem of imagination and incentives.

For shorter-duration outages, electricity users have an incentive to make their own preparations for resilience. A wide range of users do exactly that—with different levels of effort and cost depending on what they are willing to pay to avoid loss of vital services. Long-duration outages have much more profound impacts on society and require preparedness that is much more costly. Planning for such outages requires system-wide thinking because so much depends on the power grid, including all 16 critical infrastructure sectors.<sup>1</sup> As the grid becomes even more tightly integrated with other important economic and social activities, the need for this system-wide perspective will grow.

Water supply systems that provide potable water and treat wastewater are one example of critical infrastructure interdependency. Because the pumps are large, sometimes they do not have their own backup generators. Loss of grid power beyond a few hours can lead to depletion of gravity-fed reservoirs and tanks as well as a decline in pressurization of the distribution pipes. Usually the criticality of these pumps is handled through coordination with the electric distribution supplier to give those assets high priority during restoration—an option that may not be available during the

<sup>1</sup> The Department of Homeland Security designates the following 16 sectors to be critical to national security, national economics, or public health/safety: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation; and water and wastewater.

kinds of large-area, long-duration outages that are the focus of this report. Similarly, wastewater systems and particularly lift pumps are often critical if left off-line for too long. Sewage treatment often has enough storage to last for several days, but there have been cases where untreated effluent has been released directly to the environment in the aftermath of severe events.

Effective planning will require different strategies for different systems (NRC, 2012). And planning will require engaging actors—from first responders to the operators of critical infrastructures—who often do not work together adequately. Severe events and the corresponding shock, however, have inspired some of these different members of the private and public sector to work together more effectively—for example, during the aftermath of Superstorm Sandy when some parts of the tristate area lacked electric service and other infrastructure for more than a month.

This chapter looks at resilience from three perspectives: (1) incentives for actors to invest in resilience on their own, (2) planning methods that can improve how societies anticipate the effects of long-duration grid outages, and (3) approaches to designing electric power systems so they retain some or all of their function even when the larger grid has failed.

## INCENTIVES FOR PREPAREDNESS

By and large, the existing electric power grid has done a remarkable job of providing reliable electric power service. Moreover, existing users of electric power services generally have done a good job of investing where needed to make themselves more resilient when grid service is insufficient. This track record reflects the incentives at work on the actors who are relevant to planning and using grid electricity. Here the committee looks at those incentives because they help reveal places where additional efforts by industry, civil society, and government may be needed to anticipate and plan for large-scale grid outages. Such a perspective helps to expose the areas where failures to prepare are most likely—because the incentives to ensure resilience are weakest—and where additional policy action may be needed.

Surveys of existing electric power users reveal that there are huge variations in the willingness, ability, and need to pay for greater resilience; moreover, desire for resilience depends heavily on the expected duration of grid power outages. Table 5.1 shows results from one review of prior research on interruption costs of different duration and circumstances. The table is complex and busy, demonstrating huge variation (of several orders of magnitude) in the economic harm suffered by different types of customers for different types of outages. For example, the financial losses to large and medium commercial and industrial (C&I) customers are orders of magnitude larger than losses to either residential or small C&I customers. And while much is known about the impact of relatively short duration outages (<16 hours),

at present there is essentially no systematic research that provides such information for longer outages—let alone the large-area, long-duration outages that are the main subject of this study. Nonetheless, the existing research suggests that while, on the one hand, there are broader societal needs for more resilient power supply, on the other hand, cost-effective strategies must reflect that not all users need the same levels of resilience. This is particularly true for users and facilities that provide critical services such as hospitals, where using economic measures (e.g., willingness to pay) for resilient service may not be appropriate.

The incentive to become resilient is evident in the substantial investments that some power users make in obtaining backup supplies. For example, hospitals, data centers, and command posts for first responders all regularly install backup power systems. For smaller users, as well, there is extensive media coverage and advice—along with many vendor firms—that draw attention to the need for on-site power. Diesel generators are the technology of choice for this function; estimates compiled in the late 1990s suggest that the capacity of such generators in the United States was about 100 GW and growing at approximately 2 percent per year (Singh, 2001). Given the vital role of these generators in providing resilience, there has been ongoing attention to possible revision of standards for their reliability and environmental performance (Felder, 2007). There is also a substantial need for ongoing consumer education about the operation and safety of such devices since burns, fires, and especially carbon monoxide poisoning continue to be major problems.

The committee is concerned that, despite substantial investment in standby generators, awareness of the unreliability and other performance attributes of these systems remains highly uneven. According to Huber and Mills (2006), 1 percent of diesel generators at nuclear plants fail to start upon demand, while 15 percent of them fail after 24 hours of continuous operation. Consequently, nuclear sites have multiple redundant sources of backup power, and, in the wake of the Fukushima nuclear accident, the Nuclear Regulatory Commission has required additional investments in on-site power.<sup>2</sup> By contrast, the failure rates at start-up of hospital generators—which are much less well maintained in general and have fewer redundancies—are 10 times the rate of those in the nuclear industry (Mills, 2016). Similarly, there is low and uneven awareness of the challenges in obtaining fuel supplies in a long-duration outage, which presents a critical and underanalyzed risk.

**Finding:** Installing backup power systems alone is insufficient to improve resilience. These systems must be tested (i.e., started, operated) and maintained (e.g., cleaned) regularly so they function reliably during an outage. Relevant industry

<sup>2</sup> Following Fukushima, the Nuclear Regulatory Commission requires backup power for critical systems at nuclear power plants, which will likely cost the industry approximately \$4 billion (2016 dollars).

**TABLE 5.1** The Significant Variation in Estimated Financial Losses Suffered by Different Customer Classes Operating under Different Ambient Conditions as a Function of Varying Outage Duration

		Losses Based on Interruption Duration (\$)					
Timing of Interruption	Hours per Year (%)	Momentary	30 Minutes	1 Hour	4 Hours	8 Hours	16 Hours
<b>Medium and Large C&amp;I</b>							
Summer	33	16,172	18,861	21,850	46,546	96,252	186,983
Non-summer	67	11,342	13,431	15,781	35,915	77,998	154,731
Weighted Average		12,952	15,241	17,804	39,458	84,083	165,482
<b>Small C&amp;I</b>							
Summer Morning	8	461	569	692	1,798	4,073	7,409
Summer Afternoon	7	527	645	780	1,954	4,313	7,737
Summer Evening/Night	18	272	349	440	1,357	3,518	6,916
Non-summer Morning	17	549	687	848	2,350	5,592	10,452
Non-summer Afternoon	14	640	794	972	2,590	5,980	10,992
Non-summer Evening/Night	36	298	388	497	1,656	4,577	9,367
Weighted Average		412	520	647	1,880	4,690	9,055
<b>Residential</b>							
Summer Morning/Night	19	6.8	7.5	8.4	14.3	24.0	42.4
Summer Afternoon	7	4.3	4.9	5.5	9.8	17.7	31.1
Summer Evening	7	3.5	4.0	4.6	9.2	17.5	34.1
Non-summer Morning/Night	39	3.9	4.5	5.1	9.8	17.8	33.5
Non-summer Afternoon	14	2.3	2.7	3.1	6.2	12.1	23.7
Non-summer Evening	14	1.5	1.8	2.2	5.0	10.8	23.6
Weighted Average		3.9	4.5	5.1	9.5	17.2	32.4

NOTE: C&amp;I, commercial and industrial customers.

SOURCE: Sullivan et al. (2015).

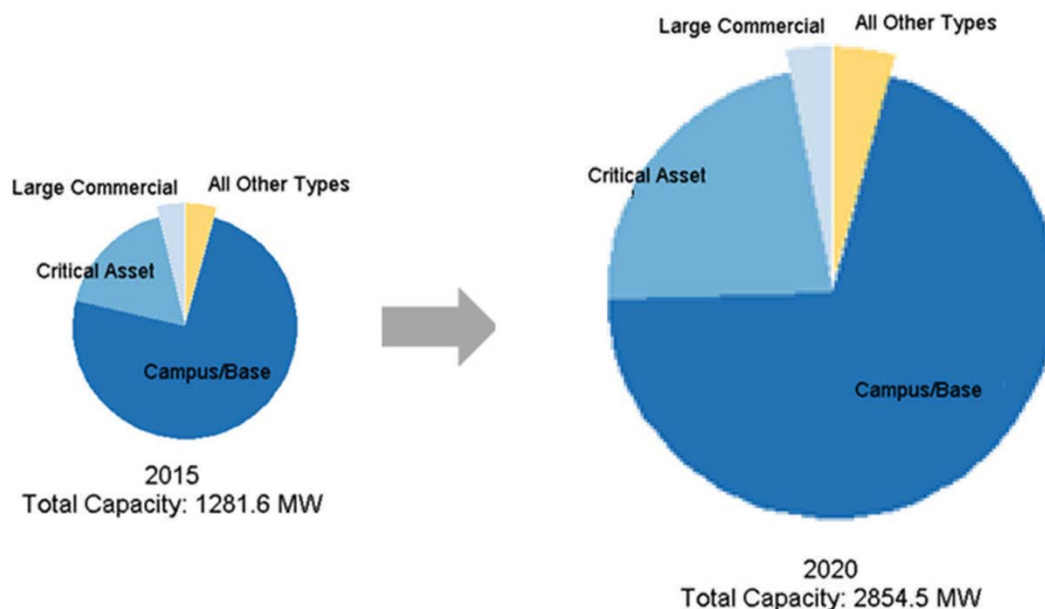
associations, and policy makers, government agencies, and regulators where appropriate, have an important role in disseminating information about the actual levels of reliability of backup units, as well as challenges obtaining fuel.

**Recommendation 5.1:** State emergency planning authorities should oversee a more regular and systematic testing of backup power generation equipment at critical facilities, such as hospitals and fire stations, and ensure that public safety officials include information related to electrical safety and responses to long-duration power outages in their public briefings. Those authorities should also periodically assess the costs and benefits of this testing program and use that information to prioritize sites for testing.

In addition to diesel generators—which are often connected to a single vital asset—there has been a steady rise in investment in microgrid systems (Hanna et al., 2017). These systems cover entire office complexes, campuses, and military bases, and, as shown in Figure 5.1, this segment of electricity infrastructure investment is expected to continue with substantial growth, which could have large implications

for the resilience of power users. While the logic for installing microgrids at such locations varies, usually the continued service of high-quality electricity even after macrogrid failure is dominant. Microgrids, especially the larger systems, are designed to allow for islanding in the event of macrogrid failure, although in practice very few actually operate or are even tested in that mode. Many microgrids embed renewable power generation systems—notably solar photovoltaics—and the financial case for larger microgrids typically hinges on the integration of natural gas-fired small turbines that utilize the waste heat for local heating and cooling. Later in this chapter, the committee will explore how new research and incentives could lead the users of microgrid systems to use this resource to increase resilience.

Over the past few years, there has also been a surge in installation of “behind the meter” on-site battery storage (see Figure 5.2 and the section titled “Near-Term Drivers of Change and Associated Challenges and Opportunities for Resilience” in Chapter 2). This surge in investment has been driven in part by direct subsidy—notably in California—and in part by fundamental improvements in battery technologies. As with microgrids, these on-site battery systems could



**FIGURE 5.1** Installation of microgrids in 2015 and expected growth to 2020.

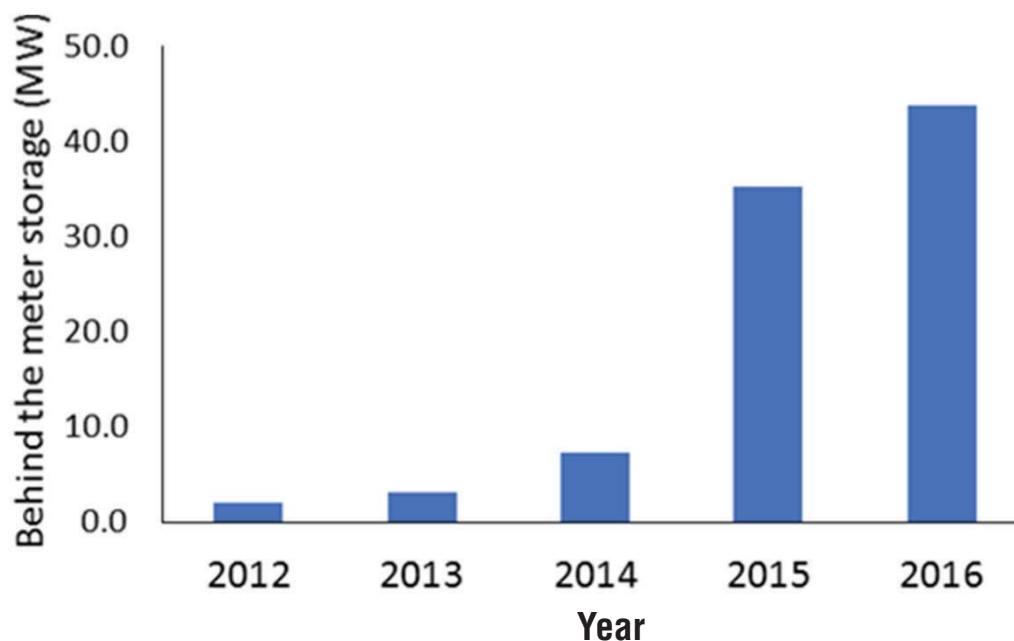
NOTE: Total U.S. electricity generation capacity in 2016 was more than 1,000 gigawatts.

SOURCE: GTM Research (2015).

in theory lead to higher resilience, but very few of these systems are actually designed for that purpose and none can supply power for periods of several days. Instead, these systems are sized to move small amounts of power—typically a fraction of total load just for an hour or two—from peak to non-peak periods to help C&I customers reduce the

charge they pay for peak electricity demand. If technological improvements make it possible to install much larger systems then such batteries could be material to improving resilience to long-duration grid outages.

Where power users have a self-incentive to invest adequately in resilience—and where they have adequate



**FIGURE 5.2** Installation of "behind the meter" battery storage systems.

SOURCE: GTM Research/ESA (2016), "U.S. Energy Storage Monitor."

**BOX 5.1****Consequences and Civic Response to Damage Caused by the Ice Storm of January 1998**

Ice storms are common in eastern Canada, with Ottawa and Montreal receiving freezing precipitation on an average of 12 to 17 days a year, but these events generally last only a few hours at a time. The January 1998 storm brought days of ice to an unexpectedly wide area of eastern Canada and the northeastern states, killing more than 40 people and causing large-scale, long-duration outages of electricity along with many other important impacts on infrastructure (NCEI, 1999).

Montreal was hit particularly hard. On January 9, much of Montreal temporarily lost its water supply after its filtration plant and pumping stations lost power (ICLR, 2013). Three out of the four major transmission lines in the area went off-line. If power had not been partially restored within hours, residents of the city would have been without potable water and firefighters would not have had water to put out fires—an outcome that forced officials to consider either evacuating the city or moving residents to facilities like Olympic Stadium, where water could be delivered by truck (Schneider, 1998). Early planning for such an outcome had not been contemplated seriously before—for example, through purchasing of on-site backup power plants—because the city had always been a priority customer of Hydro-Québec and officials thus assumed electricity would always be available (Schneider, 1998).

Even after power was restored, disruptions rippled through food supply chains, transportation, communications, and other economic activities. The storm occurred during the depths of winter and was followed by freezing weather and, 2 weeks later, by a snow storm of 8 to 16 inches that further slowed restoration (McDonnell, 1998). Along Montreal's south shore—which became known as the “triangle of darkness”—grid power remained out for 2 to 3 weeks following the storm (The Economist, 1998; Dupigny-Giroux, 2012). The commercial sector of Montreal was shut down for a week from January 9 through 16 to remove the debris and allow electrical crews to repair or rebuild the power grid in the island city (Dupigny-Giroux, 2012). Grocery stores across the area were unable to open or ran out of basic necessities, gas stations ran out of (or were unable to pump) fuel, and basic transport services were erratic—all leading to reports of a general feeling of vulnerability (Leslie, 1999; CBC, 2017; Murphy, 2009; Dupigny-Giroux, 2012; The Ottawa Citizen, 2016). All told, around 600,000 people moved out of their homes for the event, with 100,000 of them moving into temporary shelters to escape the cold (RMS, 2008). Restoration of grid services required assistance from utility crews drawn from across North America. The event prompted the largest peace time deployment of Canadian armed forces in history, with almost 16,000 troops assigned in the relief effort to help with cleanup, restoration, and evacuation.

information about the effects of their investments—no further policy incentives may be needed. By contrast, when the market fails—for example, when users are unaware of their exposure to grid failure, unaware of the synergistic consequences of grid failure, or unable themselves to afford or recoup the benefits of actions that could improve resilience if low probability events occur—then there may be a need for policy intervention. These failures are often evident where there are large-scale outages that affect a wide array of vital social services—as revealed, for example, by the long-duration power outage after the January 1998 ice storm described in Box 5.1. In contrast to many events whose intensity was predictable in ways that aided advance preparations, the extent and impact of this storm was largely unexpected. This is a characteristic of such storms since icing conditions depend critically on the vertical temperature profile in the atmosphere; a change of just a few degrees can make the difference among ice, rain, or snow. Such unexpected outcomes are particularly worrisome hazards for the grid since ice storms already account for many long-duration outages. With climate change, the areal extent and possible impacts of such icing events are likely to change although, as noted in Chapter 3, the nature of those changes remains uncertain.

The questions surrounding when and how policy makers intervene to encourage additional planning and investment around responses to grid failure raise many fundamental questions about the proper role of government. If government stands ready to provide support in the case of a long-duration grid failure, then the well-known “moral hazard” problems could undermine the incentive for users of electric power to make those investments themselves. While communities are largely left to make their own decisions about their willingness to plan for and invest in resilience, there may be broader social implications and possible unintended consequences from the totality of all these local choices made with reference to local interests.<sup>3</sup> Such societal concerns may create the need for policies to better harmonize or at least take these externalities into consideration. Indeed, better documentation and awareness of the metrics for grid reliability and resilience, discussed in earlier chapters, could make it much easier for market forces to function properly—for users of power services to become more fully aware of

<sup>3</sup> The issue of “moral hazard” arises if a community underinvests in protection for rare major events and then expects the broader society to cover its costs when such an event occurs.



their exposures to risk and thus more capable of obtaining the right level of resilience on their own.

Even once the right incentives are in place to invest in resilience, there may be organizational and cognitive barriers to action—especially for events that have never occurred or been imagined before. The committee believes that the largest challenges in creating resilience against the full effects of large-area, long-duration grid failures may lie with the system-wide consequences and interactions. Such problems are extremely difficult for organizations to anticipate and respond to effectively. Typically, organizations are structured to meet core missions and can be blind to, or find it very difficult to address, threats that arise in unexpected ways. Creating resilience against adverse system-wide effects requires that many different organizations coordinate and adopt solutions that might be far outside the normal scope of each organization individually. Where organizations do not have regular interaction and high levels of trust, collective action may be impossible.

The development of a coherent response that best serves the national interest requires laying a foundation for understanding the social value in resilience. Only then is it possible to evaluate whether the incentives of relevant actors will lead them to invest adequately in resilience. Only after establishing the social value in resilience is it possible to debate the degree of policy intervention needed to address the larger systemic impacts of large-area, long-duration outages.

**Finding:** The existing systems of incentives have generally been successful in encouraging proper levels of investment to address shorter-duration and limited-area outages. However, incentives for individuals and organizations to take steps to increase resilience against large-area, long-duration outages are a different matter. Developing national, regional, and local strategies to improve resilience against such outages requires two things: an assessment of the likelihood that disruptions will occur and a judgment about how much the various actors in society are prepared to invest in actions that lower the consequences of disruptions. At present, many communities, regulators, and grid operators do not have the information and/or incentives needed to make reasoned policy and operational decisions.

Knowing much more about what individuals and society are willing to pay to avoid the consequences of large grid failures of long duration is an important input to deciding whether and how to upgrade systems that can reduce impacts of a grid outage. Much of this knowledge is anecdotal from looking backward at such failures, such as from Hurricane Katrina, Superstorm Sandy, or the Northeast blackout of 2003. Most prior quantitative studies have only examined outages of much shorter duration. If these studies are to provide meaningful results, they will need to use state-of-the-art social science methods. Because different strategies may provide different insights, it would be prudent

to have separate independent groups undertake more than one study. Results from this work can be used to inform national, regional, and local decision making about resilience investment.

While individuals' willingness to pay is an important input to such decision making, considerations of broader social disruptions and of equity are also important. Some private actors may be willing to pay considerable amounts to assure their continued provision of electric power during events (or parts of them), but these actors typically lack incentive to make investments beyond their own needs. Others may be uninformed about the potential systemic consequences of long-duration outages. It is the role of government to assure the continued provision of critical social services and to provide access to basic power-dependent services to vulnerable groups such as disadvantaged communities or others that lack the financial mechanisms to assure their own resilience.

**Recommendation 5.2:** The National Association of Regulatory Utility Commissioners should work in coordination with the Department of Homeland Security, the Department of Energy, and the states to develop model guidance on how state regulators, utilities, and broader communities (where appropriate) might consider the equity and social implications of choices in the level and allocation of investments. These include investments in advanced control technologies capable of enabling continued supply to particular feeders or critical users that could mitigate the impacts of large-area, long-duration outages.

## PLANNING FOR GRID FAILURE

The remainder of this chapter examines how U.S. communities and the country as a whole can understand and implement an appropriate level of resilience in the event of a large outage of long duration. First, this section introduces planning for grid failure—so that consequences can be anticipated and responses organized. The following section discusses the design of infrastructures so that they themselves are more resilient to long-duration full or partial loss of grid services.

Planning requires information on the potential length and scope of large grid outages. That information can be gleaned partly by looking at past system outages and their coverage, summarized in Appendix E. These experiences suggest the magnitude of possible future outages. History in other countries is also helpful to consider because most modern grids reveal similar points of vulnerability. For example, the downtown area of Auckland, New Zealand, lost nearly all grid service for 5 weeks in the summer of 1998 when the four main cables serving the area failed in rapid succession. While each failure had its own individual causes, the events correlated and cascaded into a national crisis (Rennie, 1998).

Systems that should have been redundant instead were the source of additional stress—something that often happens in complex systems where all the interacting failure points are difficult to imagine in advance.

However, the past may be an inadequate guide because long-duration outages are rare events and the underlying structure, operation, and policies governing the grid might expose this vital infrastructure to even larger and longer outages than observed historically. It is important to do more to identify events that are “unthinkable” on the basis of historical experience but could occur with coordinated system-wide attacks on the grid and the many systems that it supports. While there are some public safety professionals and organizations that practice and train for such dark and disturbing work, these practices are neither widespread nor comprehensive enough to substantially improve the nation’s resilience to large-scale outages. Good imagination and planning begins with understanding the full range of possible outcomes for grid failure. The committee’s focus here is on planning for continuation of vital services in areas affected by a large-scale, long-duration outage, but it also notes that one important element of planning includes evacuation—in effect deciding that it may be more feasible to move populations in some areas than to provide emergency provisions.

While characterizing the real risks of grid failure will be difficult, an even more complex planning task involves understanding how prolonged full or partial failures of grid service could have compounding effects on other important public infrastructures and private services. Much of modern life depends on grid electricity, which is why the National Academy of Engineering named electricity as the single most important engineering achievement of the 20th century (NAE, 2017).

At present, planning for all types of hazards to public infrastructure is a disorganized and decentralized activity. Even in federal programs focused explicitly on increasing grid resilience, planning and implementation of research and policy responses are fragmented across federal agencies (GAO, 2017). It is impossible to describe all of the relevant efforts succinctly. Here the committee focuses on the role of the federal government and its National Preparedness System (NPS), whose broad aims are to prevent or speed recovery from a wide range of hazards that affect the security and resilience of the United States.<sup>4</sup> The NPS is organized by the Federal Emergency Management Agency (FEMA)—an arm of the Department of Homeland Security—to assess and plan for hazards to 12 vital emergency support functions, including energy, for which the Department of Energy (DOE) is responsible for primary agency support (FEMA, 2008). Table 5.2 shows the matrix of vital functions and the relevant federal agencies. It is an

intrinsically complex, messy, and organizationally stovepiped activity.

Because planning for grid failure is such an intrinsically complex and difficult task, it appears that very little of the FEMA- and DOE-led effort is devoted to imagining and preparing for the full systemic consequences of losing grid power over large areas for long period. Instead, by design, the framework shown in Table 5.2 is operational and aimed at clarifying which agencies will be focal points for receiving, collating, and distributing information to the rest of the federal government. Under this framework, for example, DOE is tasked with organizing information to produce estimates of restoration times, percentages, and priorities. In its role as the focal point, DOE is also expected to work with legal authorities to resolve matters of jurisdiction and grant waivers to expedite restoration processes, as discussed in Chapter 6. These are, for the most part, operational functions rather than forward-looking research and development or strategic planning. These patterns of stove piping and overlapping layers of jurisdiction extend from the federal to the regional, state, and local levels. Only during emergencies—events that politically and organizationally focus minds—does some semblance of more unified and strategic focus emerge, such as through the creation of joint field offices that unify the coordinating structures discussed in more detail in Chapter 6.

Because planning for the system-wide consequences of grid failure is such a daunting task, it is not surprising that the jurisdictions that seem to be doing a better job are those that have experienced such failures in the past. The tristate area of New York, New Jersey, and Connecticut in the aftermath of Superstorm Sandy is a good example, as shown in Box 5.2. Electricity outage disaster preparedness and response exercises such as “Clear Path 4” (DOE, 2016) are critical opportunities to gain experience and have great potential to be expanded. Experience transforms the unimaginable and seemingly impossible into a tangible reality. However, often the result is that planning efforts focus excessively on avoiding the same calamitous outcome rather than planning for a broader range of possible future events.

From the Sandy experience, the Canadian ice storm, and many others, it is clear that long-duration failures in grid power will occur. Even with a concerted effort in design and investment for continuity of some electric services—a topic discussed in the next section—much of the country is unprepared for long-duration outages. To the extent appropriate, resilience must begin with individual households and businesses preparing themselves for long-duration outages with adequate essential supplies—such as of food, water, medicine—to cover, at least, multi-day outages.

**Finding:** Existing planning systems are, by design, ill-suited for anticipating and considering the wide range of interactions between loss of grid power and other vital infrastructures and

<sup>4</sup> Presidential Policy Directive 8: National Preparedness. See <https://www.dhs.gov/presidential-policy-directive-8-national-preparedness>, accessed July 17, 2017.

**TABLE 5.2** The Federal Emergency Management Agency's Matrix Concept Illustrates the High Amount of Interagency and Interdepartmental Coordination Required for Assessing and Responding to Threats to the Nation's Vital Infrastructures

Department or Agency	Vital Emergency Support Functions											
	Transportation	Communications	Public Works and Engineering	Fire Fighting	Information and Planning	Mass Care	Resource Support	Health and Medical Services	USRT	HAZMAT	Food	Energy
Dept. of Agriculture	S	S	S	P	S	S	S	S	S	S	P	S
Dept. of Commerce		S	S	S	S		S			S		
Dept. of Defense	S	S	P	S	S	S	S	S	S	S	S	S
Dept. of Education					S							
Dept. of Energy					S		S	S		S		P
Dept. of Health and Human Services			S		S	S		P	S	S	S	
Housing and Urban Development						S						
Dept. of Interior		S	S	S	S					S		S
Dept. of Justice					S			S	S	S		
Dept. of Labor			S				S		S	S		
Dept. of State	S									S		S
Dept. of Transportation	P				S		S	S		S		S
Dept. of Treasury					S		S					
Dept. of Veteran			S			S	S	S				
Agency for International Development								S	S			
Administrative Resource Center					S	P		S			S	
Environmental Protection Agency			S	S	S			S		P	S	
Federal Communications Commission		S										
Federal Emergency Management Agency	S	S		S	P	S	S	S	P		S	
Government Services Agency	S	S			S	S	P	S			S	
Natl. Space and Aeronautics Admin.					S		S		S			
Natl. Clandestine Service		P			S		S	S				S
Nuclear Regulatory Commission					S					S		S
Office of Personnel Management							S					
Small Business Admin.					S							
Tennessee Valley Authority	S		S									S
U.S. Postal Service	S					S		S				

NOTE: P, principal coordinating agency; S, agencies supporting the principal coordinating agency; USRT, urban search and rescue.

SOURCE: FEMA (2008).

services for long-duration outages. These are intrinsically difficult tasks to perform both conceptually and organizationally. They require imagination and planning for interactions among multiple stresses on infrastructures and services that are rarely observed in the world.

For example, in the aftermath of a large regional storm, loss of grid power often leads to loss of reliable traffic control as well as obstruction of many roadways. These impede normal traffic flow and make it difficult for first responders to perform their tasks. The difficulties with first response,

**BOX 5.2****Superstorm Sandy: Preparation, Emergency Response, and Restoration of Services**

On October 29, 2012, Superstorm Sandy made landfall, leaving approximately 3.5 million of the 8.5 million homes and businesses in the tristate area without electricity. For 4 days prior to landfall, members of the Northeastern Mutual Assistance Group<sup>a</sup> were coordinating closely to reduce impacts and plan for restoration activities—and to reach out to other regions, such as the Midwest, to draw resources such as line crews and call center operators (EEI, 2013). Simultaneously, DOE worked to remove the red tape required for these outside crews to work in the impacted areas, as envisioned in the FEMA emergency preparedness process that had been established for the country just a year earlier (FEMA, 2013). A presidential state of emergency was declared a day before landfall, an action that further activated federal resources—such as the National Response Coordination Center (NRCC) that prepared five staging areas to preposition crews, vehicles, and 183 generators of various sizes. After landfall, as the extent of the damage became known, the NRCC also guided the Department of Defense to provide additional resources—such as airlifting 229 power-restoration vehicles and approximately 500 personnel to aid the region while the Army Corps of Engineers was tasked with pumping operations to facilitate restoration in flooded areas (FEMA, 2013). Within 2 days after landfall, 70,000 utility crewmen from around the country were working to restore the grid—by FEMA estimates, those workers replaced 4,500 poles, 2,100 transformers, 44 substations, and more than 400 miles of lines over the next 3 days (FEMA, 2013). With so many different federal agencies providing support, FEMA established the Energy Restoration Task Force on October 31 to help coordinate the federal effort—among many other functions, it coordinated the supply of 9.3 million gallons of fuel to New York and New Jersey for use by first responders and the continued operation of emergency generators (FEMA, 2013).

Since Superstorm Sandy, there have been extensive efforts by regulators and utilities to improve reliability of the grid and resilience of society—some of these efforts were triggered originally by Hurricane Irene, which hit the region the year before Sandy (FEMA, 2013). Concerning reliability, regulator orders and utility actions have identified critical power delivery systems that need hardening—such as raising the elevation of transformers at substations, adding supervisory control and data acquisition to substations, and installing equipment that will allow operators to isolate faulted areas and close circuits remotely that can keep more customers online. In the natural gas network, a massive effort has begun to replace cast iron mains and upgrade distribution systems. Public Service Electric and Gas—the largest utility in New Jersey, which saw 2 million of its 2.2 million customers lose power after Sandy—is in the midst of a regulator-approved \$1.2 billion “Energy Strong” program to protect its gas and electricity network. All told, in New Jersey alone, regulators have approved almost \$2 billion worth of investments in mitigation measures to guard against catastrophic storms and, more generally, upgrade the resilience of electric and gas systems.

Responses in New York were similar. In that state, 2.2 million customers lost power, and the two largest utilities (Consolidated Edison and Long Island Power Authority) spent \$1.2 billion to restore service while spending another \$1.7 billion after Sandy to harden their electricity, gas, and steam infrastructures.<sup>b</sup> In Connecticut, where the damage was much less relative to New York and New Jersey, relatively little federal help flowed—about 1 percent of the total federal funds spent after Sandy went to the state—and efforts focused less on recovery and hardening of infrastructure and more on helping homeowners displaced by the storm (Radelat, 2014).

Policy makers have also focused massive resources on improving resilience in the face of future power outages, although that task has required more complex coordination because few of the critical tasks for resilience map neatly onto existing policy structures. In New Jersey, the state's Board of Public Utilities in conjunction with the New Jersey Office of Emergency Management authored a Petroleum Fuel Task Force Plan. The New Jersey Board of Public Utilities is the lead agency for administering this new plan, which is intended to address fuel shortages or disruptions to the fuel distribution system in times of an emergency. More than 125 gas stations throughout the state have been equipped with emergency generators or electrical connections to accept a portable generator.

<sup>a</sup>Every region of the country has such mutual assistance groups.

<sup>b</sup>For regulatory action after Sandy, see, e.g., Cases 13-E-0030, 13-G-0031, and 13-S-0032 of the New York Department of Public Service.

in turn, magnify the humanitarian crises that result from the original storm event. Those difficulties compound into additional stresses on hospitals and public safety that consume their resources and make it more difficult to restore normal commercial operations. But even in such settings, it can be extremely difficult to anticipate how interactions among infrastructures lead to yet further interactions and harmful consequences that multiply as a grid outage event extends in time.

State and local emergency management organizations may not have sufficient understanding of electric power systems, which can slow down emergency power provision to critical facilities. In some states, such as California, organizations such as the California State Utility Emergency Association act as a liaison between critical infrastructure utilities and emergency management organizations. While several other states have similar programs, the practice is not widespread.

**Finding:** In every state, the governor is the ultimate authority responsible for overseeing disaster recovery and the mobilization of federal assistance. However, the states vary widely in the extent to which they are ready to perform these functions for long-duration grid outages. State and regional authorities would benefit from extending existing efforts to help identify common challenges and extend best practices—for example, the National Association of State Energy Officials' efforts to improve awareness and preparedness for large-scale disruptions to energy infrastructure (e.g., by holding events to share best practices and experiences managing fuel shortages that often accompany grid outages and other infrastructure failures [NASEO, 2016]).

The technology of distribution system operations increasingly allows power system operators, in the face of limited grid or local power supply, to select which distribution feeders to energize. Those feeders typically serve loads with very different levels of social criticality, such as hospitals or water treatment plants. Advanced control will make it possible to selectively supply and/or restore power to individual meters on a feeder, with subsequent or sequenced restoration of service to others on that feeder. It will also be possible to change the allocation of which meters to supply over time as circumstances and needs evolve. While presently there are relatively few demonstration projects and microgrids with these functionalities, there is significant potential to improve resilience through their wider adoption.

**Finding:** Technologies that allow for intelligent, adaptive islanding of the distribution system create new needs for planners to envision which feeders and users should be energized under different circumstances. Yet, that type of planning has been minimal, and little effort has been dedicated to anticipating how energizing feeders and select users might be adapted over the lifetime of the outage.

**Recommendation 5.3:** We recommend that the Department of Homeland Security, and the Department of Energy, as the energy sector-specific agency, develop and oversee a process to help regional and local planners envision potential system-wide effects of long-duration loss of grid power. While orchestrated at the federal level, success of this effort will require sustained engagement by regional and local authorities. Federal seed funding could support several such local or regional assessments.

Officials in regions that have experienced long-duration outages will likely be more motivated (see Box 5.2). In other regions, the Department of Homeland Security and others will need to mobilize support for taking these “imagine the unimaginable” activities seriously. The regulatory community's role in these efforts will be crucial. Public utility regulators in particular often have oversight over many

infrastructures and determine whether electric utilities may recover the costs associated with planning for the effects of long-duration outages of grid power.

**Recommendation 5.4:** The National Association of Regulatory Utility Commissioners, in consultation with the Department of Energy, the Department of Homeland Security, and the states, should develop guidance to state regulators and utilities on the following: (1) selective restoration options as they become available, (2) the factors that should be considered in making choices of which loads to serve, and (3) model recommendations that states and utilities can build upon and adapt to local circumstances. In developing these recommendations, attention should be paid to how the use of these new technical capabilities to energize particular feeders or grid-connected users might create evidence to justify wider deployment of such control and metering technologies.

Examples of factors that such guidance might consider include the power needs of first responder and other critical infrastructure systems, service to selected fuel and food suppliers, availability (or lack thereof) of privately supplied backup generation or other means to assure continued availability of electricity, and ability of specific populations to access basic services during prolonged outages.

The industry has done extraordinarily well at improving how the country responds to existing grid failures, a topic explored in more detail in Chapter 6. That said, a great deal of the effort needed to imagine and plan for the effects of long-duration outages sits outside the power industry in other organizations—such as the operators of water supply and treatment facilities and first responders. But industry, led by the North American Electric Reliability Corporation (NERC), should take a fresh look at whether the existing system of reliability standards adequately envisions cascading effects that could lead to long-duration outages. And the industry's central strategic organizations—notably the Edison Electric Institute, the American Public Power Institute, the National Rural Electric Cooperative Association, and NERC—should draw more attention to the need for society to plan for long-duration outages. This is important, even though such tasks may be uncomfortable for these organizations because they represent, to some degree, an awareness that the grid itself is more fragile than widely thought. At the same time, such self-driven industry efforts should improve awareness of the many ways that the grid system can be designed to allow more resilience, which is an area where there are highly varied experiences across existing U.S. utilities and other system operators.

Finally, much more attention is needed to engage the public in understanding the potential severity of large-area, long-duration blackouts and to improve public awareness and preparedness. The American Red Cross (2016) offers general guidance on how to prepare for power outages—with



supplies adequate for 3 days (assuming evacuation from home) or up to 2 weeks (assuming that homeowners stay at home). The Centers for Disease Control offer detailed guidance on food safety, noting that hazards to refrigerated food begin as early as 4 hours into a prolonged power outage; they also offer rudimentary strategies for disinfecting water (CDC, 2014). Many states also offer their own guidance tailored to local hazards—for example, Florida's advice focuses on the need for 3 days of supplies to ride through outages caused by hurricanes (Harrison, 2016). It is unclear how households around the nation respond to this advice, or what factors may drive households to achieve appropriate levels of preparedness. FEMA assesses individual preparedness on a regular basis, and the results suggest that preparedness is low and not improving rapidly (FEMA, 2016). Similarly, many households and businesses obtain equipment—such as portable generators—yet are unaware of how to operate these devices safely, how to procure fuel during extended outages, and how low the real levels of reliability of these devices are in practice.

## DESIGN

With better understanding of what society might be willing to pay to avoid or reduce the consequences of grid failure and equipped with better planning for how grid failure could affect other critical infrastructures, planners could then design systems so they are more resilient when grid power is lost. The committee looks at design from two related perspectives: (1) designing and deploying standby power systems, and (2) designing local power systems to provide higher customer resilience.

### Designing and Deploying Standby Power Systems

Many methods already exist to establish on-site power systems—often using components that are patched together in ad hoc ways—that can provide local service in the event of grid failure. These existing approaches should be practiced and improved. Most backup power systems rely on small gasoline, natural gas, and diesel-fired generators that are relatively easy to operate. Nonetheless, experience operating these systems is highly uneven around the country. Areas in which loss of grid power is more frequent are, as a general rule, better at imagining the impacts and thus better prepared.

These self-supplied systems may be ineffective in the case of long-duration, large-scale interruptions because backup systems are generally designed to run reliably for a few days at most; after that point, maintenance and fueling may be essential. However, during a large event that affects many interconnected public infrastructures, such services may be very challenging to obtain. During such outages, households and other non-expert users often devise their own ad hoc solutions that can lead to adverse side effects—for example, carbon monoxide poisoning from small generators run with

inadequate ventilation. Better information and oversight are needed to improve the availability, safety, and use of these power systems.

Many (if not most) of the emergency generators are not physical assets owned by government or even utilities. Instead, the government maintains contracts with the private sector to deliver equipment as needed. For example, the federal government maintains a small stockpile of portable generators at locations around the country, as well as much larger contracts for additional procurements that can be deployed during a major outage. It is poorly understood whether many of the contracts for provision of generators, fuel, and maintenance would prove to be robust under conditions that lead to sustained loss of grid power—conditions that might include natural disasters and cascading interactions between infrastructures under stress. For example, where delivery of these assets is envisioned by air, supporting facilities (e.g., airports, ground crews, and air traffic control) may be unavailable and roads may be impassable.

In addition to the contracts and stockpiles of mobile generators maintained by the federal government, there is potential to repurpose assets not traditionally used for power supply. Civilian and navy ships could provide a few tens of megawatts of emergency power to loads in coastal cities (Scott, 2006). Likewise, when they are equipped with appropriate interfaces or conversion kits, diesel electric locomotives can also be used to power communities located near railroad tracks. For example, Canada National Railway delivered multiple locomotives off-track to towns without power during the 1998 ice storm.

There are several other anecdotes of locomotives being used to supply power to critical loads during emergencies, and many train operators maintain conversion kits used to produce 60 Hz of alternating current power from locomotives. However, the availability of such conversion kits is likely limited, and it remains unclear how much load such non-traditional sources of emergency power could serve during actual blackout conditions (NRC, 2012). Nonetheless, such resources can augment federal emergency power operations that rely on conventional mobile generators.

**Finding:** The federal government maintains a small stockpile of portable generators and fuel, as well as contracts for additional procurements that can be deployed during a major outage. However, the quantity available in the event of a large outage is inadequate, probably by a large margin, and likely to remain that way. Furthermore, there is a lack of knowledge regarding the existence, load characteristics, and emergency power requirements of many critical facilities. During emergency operations, this can impede procurement, delivery, and installation of the proper equipment at the site. Also unknown is the ability to reliably obtain non-traditional sources of emergency power such as from train locomotives and ships.

**Recommendation 5.5:** The Department of Energy and the Department of Homeland Security should evaluate and recommend the best approach for getting critical facility managers to pre-register information about emergency power needs and available resources. Collecting this information in a centralized, accessible database will expedite provision of emergency power to critical facilities and help set priorities for allocating resources. The Emergency Power Facility Assessment Tool managed by the U.S. Army Corps of Engineers—a tool already in use but whose adequacy the committee was unable to assess completely—may prove to be a suitable platform. Once these informational resources are in place, periodic stress testing and evaluation are needed to ensure that they continue to provide reliable information.

It is crucial to increase community assessments of what will and will not work in the event of large outages of varying duration (including availability of liquid fuel and generators; power to refineries, gas stations, communication networks, and hospitals; local and regional availability of natural gas; workforce). These should be integrated with tabletop emergency planning exercises at the community, county, and state levels. FEMA provides some funding for state and local exercises. However, resilience to large-area, long-duration outages may not be adequately prioritized in existing state/local exercises, and greater emphasis could produce good models for systematic planning and operational assessments.

### Designing Local Power Systems to Provide Higher Customer Resilience

Beyond customer-owned sources of backup power, the power infrastructure, and distribution systems in particular, could be designed to operate more effectively when the bulk transmission parts of the grid fail. Many utilities are already installing self-healing and self-correcting distribution systems. These have ubiquitous sensors that can identify and isolate faults and use automated or remotely controlled switching to assure continuity of power to as many users as possible. For purposes of this chapter, what is important about these systems is that they blur the lines between reliability and resilience. When they work effectively, these automated distribution systems improve reliability of traditional grid service. But it is a small step to extend that logic to integration of electric infrastructure that is located on a customer's premises—for example, an intelligent microgrid that can island from or reconnect to the larger system as conditions require. Other examples include on-site battery storage at customers' residences, which combined with photovoltaics (PVs) could provide continuity of service in the event of grid failure (i.e., reliability) and also offer local support for the grid that can help avoid outages or expedite restoration (i.e., resilience). In terms of grid design and decentralization, these activities at the "edge" of the traditional grid are important technological and behavioral frontiers for the future

power system. At present, most of the capabilities—such as automated islanding and intelligent integration of local resources into utility distribution systems—are theoretical in nature and have not been tested at scale.

A particularly promising set of options related to improving resilience rests with various types of microgrids. It is crucial to understand how microgrids can enhance resilience by operating in self-islanding mode during long periods of grid failure. In that context, there are various classes of microgrids:

- *Building scale.* Nanogrids are small-scale microgrids feeding residential or commercial end users. During an outage, the nanogrid typically isolates from the distribution system, and individual energy resources (e.g., a rooftop PV system with battery energy storage, a local diesel generator, or a fuel cell) are used to power the local loads. At present, most of these small self-supply systems serve the purposes of improving reliability and saving customers' money through self-generation. Most of these systems are not designed to provide reliability for long-duration outages of the macrogrid, and many of these systems (e.g., at the residential level) are not designed to operate in islanded mode at all. Technically, however, many more of these systems could be designed with those capabilities.
- *Campus scale.* Microgrids are emerging as solutions for whole collections of buildings (e.g., college campuses or military facilities). All of these systems are designed with the capability of seamlessly connecting and disconnecting (i.e., islanding) from the macrogrid. Maintaining power at these locations—oases during emergency situations may be critical for safely riding through a catastrophic event. This is the fastest growth segment of microgrids in part because there are some customers willing to pay heavily for reliability (e.g., military bases) and in part because large-scale energy users can take advantage of combined heat and power efficiencies from burning natural gas in micro turbines (Hanna et al., 2017). For these latter users, dependence on natural gas supplies—which themselves may be compromised during events that lead to outage of the macrogrid—may be an extra source of vulnerability. Earthquakes that affect the power grid can also disrupt natural gas supplies. Extreme cold associated with ice storms can spike other demands for gas, such as heating, and leave less gas for power generation. Such systems, in many cases, are designed for islanding within the microgrids—so that critical services such as hospitals and sensitive scientific equipment are kept online even as the rest of the microgrid suffers graceful degradation in service.
- *Community scale.* Community-centric microgrids can be established by sharing individual end users' distributed energy resources (DERs)—a capability that exists

in principle but, so far, is rarely observed in reality. This functionality remains socially and technically challenging, as there are issues with safety, protection, controls, and metering.

**Finding:** There is enormous technical potential to using microgrids to make electric service more resilient in the face of loss of bulk grid power. This field of research and application is evolving quickly with new control systems, sensors, and distributed energy resources. This rapid evolution of the frontier of technical capabilities is opening a potentially wide gulf between the technical capabilities of microgrid systems and the real-world systems that are operational.

It is difficult to test microgrids and self-islanding distribution systems in real failure modes, especially if real-world events that lead to grid failure create many other forces that could erode the capabilities of self-islanded or microgrid systems. Variations in power quality could damage sensitive equipment needed for operation of these systems, as could physical stresses (e.g., trees, water, wind) that are correlated with the larger events that caused macrogrid failure in the first place. Too little is known about whether decentralization of the power grid will improve or degrade resilience of service under varying conditions. A highly decentralized and automated grid system that is still controlled by central authorities could prove to be a highly effective means of assuring resilient energy services even in the face of macrogrid failure. Or decentralization could actually amplify vulnerabilities in the grid system. Control systems may be unable to provide stability in the face of large numbers of local decisions made without the benefit of centralized authorities. Those systems might also fail in coordinated ways—for example, in case of cyber attack on the power infrastructure.

**Finding:** Many microgrids have been designed with continuous grid integration in mind, and users are hesitant to operate them in abnormal modes (e.g., islanded, or back-feeding power to the local utility) that could cause harm. Too little is known about whether decentralization of the power grid will improve or degrade resilience of service under varying conditions. A highly decentralized and automated grid system that is still controlled by central authorities could prove to be a highly effective means of assuring resilient energy services even in the face of macrogrid failure. Or, decentralization could actually amplify the vulnerabilities in the grid system.

**Recommendation 5.6:** The Department of Energy should support demonstration and a training facility (or facilities) for future microgrids that will allow utility engineers and non-utility microgrid operators to gain hands-on experience with islanding, operating, and restoring feeders (including microgrids). While the full need for training and experience—as well as possible adjustment in microgrid standards,

notably those developed by consensus under the Institute of Electrical and Electronics Engineers (e.g., 1547.4 and the 2030 family of standards, which are, at this writing, under revision)—is large, the committee envisions a small Department of Energy-backed program to establish best practices that could spread more widely across industry and the regulatory community.

As discussed in Chapter 2, today, in most states, regulatory and legal restrictions limit the ability of a microgrid to sell power to other entities or to move power across public thoroughfare unless it is operated by a traditional electric utility. At smaller scale, privately owned microgrids could offer significant advantages, even with existing rate structures that typically do not acknowledge the value such a system can provide to the grid (King and Morgan, 2007).

## DISTRIBUTION SYSTEM INNOVATIONS THAT COULD ENHANCE RESILIENCE

Today when the power goes out, individual customers are essentially on their own until service is restored. Homes and commercial facilities that are equipped with standby generators can disconnect from the grid and continue to operate with full or partial power. Users with microgrids—such as some campuses and military bases—can island from the grid and continue operations. Everyone else, even those customers with grid-connected PV systems, finds themselves in the dark. There are ways to enhance local resilience, such as by making PV inverters more visible and controllable, by facilitating development of small private microgrids, and by enabling utilities to operate islanded feeders.

### Increasing the Capabilities of Distributed Energy Resource Inverters

End users and utilities are investing in a wide array of DERs (e.g., PV arrays, wind turbines, battery storage), many of which are located on or near customers' premises. These resources could be used, in theory, to provide power to local loads even when the grid is unavailable. Typically, these local resources are interconnected with the grid through power electronic devices called inverters that convert the direct current output from many of these devices into alternating current. Integrating these resources into the grid has presented regulatory and technical challenges. Currently, these devices are required to automatically disconnect when the voltage and/or frequency at their terminals deviates outside of a normal range, indicating the presence of a fault somewhere on the grid. There are several reasons for this requirement, including safety of the line crews in the field and protection of equipment. However, because of the way inverters and their control systems are now implemented, this also results in cutting off the supply of power to the DER owner as well as to the grid. Given the rapidly increasing penetration of

DERs, it may often be desirable to keep these resources online during abnormal situations. Motivated by concerns related to the stability of the bulk power system, FERC has modified its small generator interconnection regulations to require that DERs have the ability to “ride through” momentary fluctuations of frequency or voltage.<sup>5</sup> In addition, the Institute for Electrical and Electronics Engineers is in the process of revising DER interconnection standards (IEEE, 2014), including guidelines for the intentional formation and operation of microgrids. These developments could have a positive impact on resilience during large-scale outages.

While it is not yet deployed at significant scale, technology is readily available to allow inverters to power local loads following automatic grid disconnection, making limited local power available to run refrigerators, freezers, and other critical loads.<sup>6</sup> In addition to increasing resilience and reliability for end-use customers, ongoing advances in inverter technology and modifications to interconnection regulations can be beneficial for keeping local loads at least partially energized during large-area, long-duration outages. Such advances can also be beneficial for utilities during restoration (see Chapter 6). With proper design and operating standards, DERs and advanced inverters could actively contribute to the stability and reliability of microgrids to power local loads without jeopardizing equipment or human safety. Nevertheless, individual states are in various stages of policy development related to inverter performance and interconnection of DERs.

**Recommendation 5.7:** Utility regulators and operating utilities that have not adopted standards similar to the Federal Energy Regulatory Commission’s ride-through capability requirements for small generators should assess their current interconnection standards as applicable to distributed energy resources, consider the costs of requiring new installations to use enhanced inverters, and determine the appropriate policy for promoting islanding and other related capabilities.

### Encouraging Private Microgrids

As explained in Chapter 2, in most states today, regulatory arrangements and laws granting distribution utilities exclusive service territories preclude private entities from constructing and operating microgrids if done in a manner that supplies power to an entity other than the owner of the microgrid or if that power is moved across a public thoroughfare. However, because many distributed generation (DG) systems display economies of scale (King, 2006), there may be sound economic justifications for customers to want

to operate some privately owned microgrids at a scale that serves several customers. Indeed, the military does this on many bases, at times with reliability benefits for non-military users as well. Microgrids have several advantages for the electricity grid; for example, they can provide electricity during peak-usage hours and therefore forestall the need for expensive upgrades in central generation, transmission, and distribution systems. They can also be used to improve power quality and reliability for local consumers (Neville, 2008). Finally, with proper arrangements they can serve local customers during power outages, consequently increasing the resilience of the grid. A potential advantage of facilitating the development of privately owned and operated microgrids is that this could considerably speed the pace of innovation (in much the way innovation was spurred after deregulation in the telecom industry).

**Recommendation 5.8:** The Department of Energy should work with the National Association of Regulatory Utility Commissioners and state regulators to undertake studies of the technical, economic, and regulatory changes necessary to allow development and operation of privately owned microgrids that serve multiple parties and/or cross public rights-of-way. These studies should also consider the potential consequences of such changes.

**Recommendation 5.9:** State legislatures and public utility commissions should explore economic, ratemaking, and other regulatory options for facilitating the development of private microgrids that provide resilience benefits. Rate structures can be developed to cover the costs of upgrading and maintaining grid assets while also recognizing and rewarding the benefits that distributed energy resources provide to the grid.

### Facilitating Utility-Operated Islanded Feeders

Traditional radial distribution feeders are designed only to move power from substations out to customers in one direction. More modern distribution systems that include distribution automation and intelligent bi-directional sectionalizing switches,<sup>7</sup> and other advanced distribution technologies, such as smart meters and micro-phasor measurement units, can reconfigure distribution system topology and feed distribution circuits from more than one location (Grijalva and Tariq, 2011; Grijalva et al., 2011). As the amount of utility and privately operated DG<sup>8</sup> on distribution systems grows, there is no technical reason why, during an extended

<sup>5</sup> FERC Order No. 828, 81, Fed. Reg. 50,290, 156 FERC ¶ 61,062 (2016).

<sup>6</sup> See, for example, the Outback FX 2.5kW 120VAC 24VDC 55A Sealed Inverter/Charger GTFX2524 from CivicSolar: <https://www.civicsolar.com/product/outback-gtfx2524-sealed-grid-tie-24v-25kw-inverter>, accessed July 13, 2017.

<sup>7</sup> See, for example, the IntelliRupter® PulseCloser® Fault Interrupter from the S&C Electric Company: [http://www.sandc.com/en/products-services/products/intellirupter-pulsecloser-fault-interrupter/](http://www.sandc.com/en/products-services/products/intellirupter-pulsecloser-fault-interrupter/http://www.sandc.com/en/products-services/products/intellirupter-pulsecloser-fault-interrupter/), accessed July 12, 2017.

<sup>8</sup> DG is a subset of DERs. DERs can include storage and non-generation resources.



outage, an intact distribution feeder could not be operated as an islanded micro-grid, supplying customers with limited critical electric service (Narayanan and Morgan, 2012). However, progress will be needed on a variety of technical and regulatory fronts. For example, as DG resources grow in size, simple “plug and play” arrangements are no longer feasible because issues of stability, as well as frequency and voltage control, become critical (Nazari et al., 2012; Nazari et al., 2013). Distribution systems with smart meters can drop customers before reconfiguring as an island, but issues of synchronizing DG resources and assuring adequate stability also need to be addressed (Nazari and Ilic, 2014). In most cases, it is unlikely that the amount of power available to an islanded feeder would be sufficient to meet all local loads. That means that methods would need to be developed to limit the load imposed by individual customers and perhaps to cycle supply among customers over time. Any operation of islanded feeders using DG resources must be planned and executed in a fashion that does not create a safety hazard for residents or utility repair crews.

Today, an inability to observe the details of what is going on (i.e., lack of visibility) in distribution systems is a significant technical barrier to the islanded operation of DGs and microgrids. Generally, this issue is lessened in transmission systems, as transmission systems typically have greater visibility. During a power outage, transmission system operators can often readily and accurately identify most fault(s) and isolate them from the rest of the grid. Thus, the rest of the system can continue its normal operation while line crews work to repair the isolated part of the grid in a safe manner. If utilities undertake a similar approach for distribution systems and implement smart meters and micro-phasor measurement units in distribution systems, or at least at the points of interconnection of DGs/microgrids, they can identify energized lines during outages and isolate them to ensure line crew safety, while serving critical loads.

**Recommendation 5.10:** Utilities that have already implemented smart meters and advanced distribution systems with sectionalizing switches should explore the feasibility of establishing contractual and billing agreements with private owners of distributed resources and developing the ability to operate intact islanded feeders as islanded microgrids powered by utility- and customer-owned generating resources to supply limited power to critical loads during large grid outages of long duration.

**Recommendation 5.11:** Utility regulators and non-governmental entities should undertake studies to develop guidance on how best to compensate the owners of distributed generation resources who are prepared to commit a portion of their distributed generation capacity to serve islanded feeders in the event of large outages of long duration. Additionally, the National Association of Regulatory Utility Commissioners

should establish a working group to advise members on the issues they will likely have to address as the possibility grows that some utilities or customers may wish to be able to operate islanded feeders during large outages of long duration.

### Facilitating Emergency Use of Hybrid and Fuel Cell Vehicles for Backup Power

With appropriate inverters, plug-in hybrid electric vehicles and fuel cell vehicles are effectively mobile generators that customers could use to provide emergency power to critical loads in their homes, and in theory to an islanded feeder, during a major outage. Like other mobile generators, this service depends on continued availability of fuel, whether natural gas, gasoline, or something similar. Battery electric vehicles with no combustion system only store modest amounts of energy (i.e., 80 kWh at the high end), which would likely be exhausted early in the course of a large-area, long-duration outage. Thus, purely electric vehicles do not offer the same level of resilience benefit for homeowners but could be coupled with DG such as PVs. Inverters designed for vehicle-to-home power transfer have not entered the market in the United States, although there are numerous demonstration projects, in part because of technical, economic, and liability questions that must be negotiated among grid operators, homeowners, and vehicle manufacturers.

**Recommendation 5.12:** The Department of Energy should work with the manufacturers of plug-in hybrid electric and fuel cell vehicles to study how such vehicles might be used as distributed sources of emergency power.

## REFERENCES

- American Red Cross. 2016. “Power Outage Safety.” <http://www.redcross.org/get-help/prepare-for-emergencies/types-of-emergencies/power-outage/#Prepare-in-Advance>. Accessed July 11, 2017.
- Briggs and Stratton. 2015. “Briggs & Stratton Corporation Harris Poll Survey: How Homeowners Prepare for Power Outages.” [https://www.briggsandstratton.com/na/en\\_us/news-room/basco-harris-poll-survey-regarding-power-outages.html](https://www.briggsandstratton.com/na/en_us/news-room/basco-harris-poll-survey-regarding-power-outages.html). Accessed May 31, 2015.
- CBC (Canadian Broadcasting Corporation). 2017. “The Ice Storm of 1998.” <http://www.cbc.ca/archives/topic/the-ice-storm-of-1998>. Accessed March 30, 2017.
- CDC (Centers for Disease Control and Prevention). 2014. “Natural Disasters and Severe Weather.” <https://www.cdc.gov/disasters/poweroutage/needtoknow.html>. Accessed May 31, 2017.
- DOE (Department of Energy). 2016. *Clear Path IV Energy-Focused Disaster Response Exercise: Exercise Summary Report*. [https://energy.gov/sites/prod/files/2016/08/f33/ClearPathIV\\_Exercise%20Summary%20Report\\_Public%20Release.pdf](https://energy.gov/sites/prod/files/2016/08/f33/ClearPathIV_Exercise%20Summary%20Report_Public%20Release.pdf).
- Dupigny-Giroux, L.A. 2012. USA impacts and consequences of the ice storm of 1998 for the North American north-east. *Weather* 55(1): 7–15.
- Eaton. 2016. *Blackout Tracker: United States Annual Report*. [http://images.electricalsector.eaton.com/Web/EatonElectrical/%7Bc9381362-7f37-4a86-921f-83e72e8792e1%7D\\_Blackout\\_Tracker\\_US\\_2016\\_Annual\\_Report.pdf](http://images.electricalsector.eaton.com/Web/EatonElectrical/%7Bc9381362-7f37-4a86-921f-83e72e8792e1%7D_Blackout_Tracker_US_2016_Annual_Report.pdf).



- EEI (Edison Electric Institute). 2013. "Mutual Assistance." <http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Pages/default.aspx>. Accessed December 15, 2016.
- Felder, F.A. 2007. *New Performance-Based Standards for Standby Power: Re-examining Policies to Address Changing Power Needs*. <http://www.cleaneenergy.org/wp-content/uploads/New-Performance-based-Standards-for-Standby-Power.pdf>.
- FEMA (Federal Emergency Management Agency). 2008. *Emergency Support Function Annexes: Introduction*. [https://www.fema.gov/media-library-data/20130726-1825-25045-0604/emergency\\_support\\_function\\_annexes\\_introduction\\_2008\\_.pdf](https://www.fema.gov/media-library-data/20130726-1825-25045-0604/emergency_support_function_annexes_introduction_2008_.pdf). Accessed July 11, 2017.
- FEMA. 2013. *Superstorm Sandy After Action Report*. [https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy\\_fema\\_aar.pdf](https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf).
- FEMA. 2016. "Research: Citizen Preparedness Surveys Database." <https://www.ready.gov/research>. Accessed July 11, 2017.
- GAO (Government Accountability Office). 2017. *Electricity: Federal Efforts to Enhance Grid Resilience*, GAO-17-153. <https://www.gao.gov/assets/690/682270.pdf>.
- Grijalva, S., and M.U. Tariq. 2011. Prosumer-based smart grid architecture enables a flat, sustainable electricity industry. In *Innovative Smart Grid Technologies*. Proceedings of the IEEE Power and Energy Society General Meeting, Anaheim, Calif., Jan 17–19.
- Grijalva, S., M. Costley, and N. Ainsworth. 2011. Prosumer-based control architecture for the future electricity grid. In *Control Applications*. Proceedings of the IEEE International Conference on Control Applications, Denver, Colo., September 28–30.
- GTM Research (Greentech Media Research). 2015. *North American Microgrids 2015: Advancing Beyond Local Energy Optimization*. <https://www.greentechmedia.com/research/report/north-american-microgrids-2015>. Accessed July 17, 2017.
- GTM/ESA (Energy Storage Association). 2016. "U.S. Energy Storage Monitor." <https://www.greentechmedia.com/research/subscription/u.s.-energy-storage-monitor>. Accessed July 17, 2017.
- Hanna, R., M. Ghonima, J. Kleissl, G. Tynan, and D.G. Victor. 2017. Evaluating business models for microgrids: Interactions of technology and policy. *Energy Policy* 103: 47–61.
- Harrison, C. 2016. "The Essential Guide to Hurricane Preparedness." <http://www.stateofflorida.com/articles/hurricane-preparedness-guide.aspx>. Accessed December 30, 2016.
- Huber, P., and M. Mills. 2006. *The Bottomless Well: The Twilight of Fuel, the Virtue of Waste, and Why We Will Never Run Out of Energy*. New York: Basic Books.
- ICLR (Institute for Catastrophic Loss Reduction). 2013. "Ice Storm 98: An Ice Storm Chronology." <http://www.iclr.org/icestorm98chrono.html>. Accessed December 30, 2016.
- IEEE (Institute for Electrical and Electronics Engineers). 2014. *IEEE 1547 Standard for Interconnecting Distributed Resources with Electric Power Systems*. [http://grouper.ieee.org/groups/sc21/1547/1547\\_index.html](http://grouper.ieee.org/groups/sc21/1547/1547_index.html). Accessed July 11, 2017.
- King, D.E. 2006. Electric Power Microgrids: Opportunities and challenges for an emerging distributed energy architecture [PhD Thesis]. Carnegie Mellon University, Pittsburgh, Pa.
- King, D.E., and M.G. Morgan. 2007. Customer-focused assessment of electric power microgrids. *Journal of Energy Engineering* 133:3.
- Leslie, J. 1999. "Powerless." *Wired Magazine*, April 1. <https://www.wired.com/1999/04/blackout/>. Accessed July 11, 2017.
- McDonnell, S. 1998. "Diary of a Disaster: 1998 Ice Storm." <http://www.imiuru.com/icestormdiary/1pages/MoreDiary.html>. Accessed December 15, 2016.
- Mills, M. 2016. *Exposed: How America's Electric Grids are Becoming Greener, Smarter, and More Vulnerable*. New York: Manhattan Institute.
- Murphy, R. 2009. *Leadership in Disaster: Learning for a Future with Global Climate Change*. Québec, Canada: McGill-Queens University Press.
- NAE (National Academy of Engineering). 2017. "Greatest Engineering Achievements of the 20th Century." <http://www.greatestachievements.org/>. Accessed July 13, 2017.
- Narayanan, A., and M.G. Morgan. 2012. Sustaining critical social services during extended regional power blackouts. *Risk Analysis* 32: 1183–1193.
- NASEO (National Association of State Energy Officials). 2016. "Western Regional Emergency Fuel Coordination Meeting." <http://www.naseo.org/event?EventID=1435>. Accessed July 11, 2017.
- Nazari, M.H., and M. Ilic. 2014. Dynamic modelling and control of distribution energy systems: Comparison with transmission power systems. *The Institution of Engineering and Technology Generation, Transmission, and Distribution* 8(1): 26–34.
- Nazari, M.H., M. Ilic, and J.P. Lopes. 2012. Small-signal stability and decentralized control design for electric energy systems with large penetration of distributed generators. *Control Engineering Practice* 20(9): 823–831.
- Nazari, M.H., M. Ilic, and M.G. Morgan. 2013. "Toward Model-based Policy Design for Reliable and Efficient Integration of Distributed Generators." Presented at the IEEE PES General Meeting, Vancouver, British Columbia, July.
- NCEI (National Centers for Environmental Information). 1999. "Eastern U.S. Flooding and Ice Storm." <https://www.ncdc.noaa.gov/oa/reports/janstorm/janstorm.html>. Accessed December 15, 2016.
- Neville, A. 2008. "Microgrids Promise Improved Power Quality and Reliability." *Power Magazine*, June 15. <http://www.powermag.com/microgrids-promise-improved-power-quality-and-reliability/>. Accessed February 8, 2017.
- NRC (National Research Council). 2012. *Terrorism and the Electric Power Delivery System*. Washington, D.C.: The National Academies Press.
- Radelat, A. 2014. "Feds give Connecticut relatively little for recovery from Sandy." *CT Mirror*, June 20. <http://ctmirror.org/2014/06/20/feds-give-connecticut-little-to-recover-from-sandy/>. Accessed July 11, 2017.
- Rennie, H. 1998. "Auckland Power Supply Failure." <https://web.archive.org/web/20090307230605/http://www.med.govt.nz/templates/Page12136.aspx>. Accessed December 15, 2016.
- RMS (Risk Management Solutions). 2008. *The 1998 Ice Storm: 10-Year Retrospective*. [http://forms2.rms.com/rs/729-DJX-565/images/wtr\\_1998\\_ice\\_storm\\_10\\_retrospective.pdf](http://forms2.rms.com/rs/729-DJX-565/images/wtr_1998_ice_storm_10_retrospective.pdf).
- Ryan, B., R.C. Franklin, F.M. Burkle, P. Aitken, E. Smith, K. Watt, and P. Leggat. 2015. Identifying and describing the impact of cyclone, storm and flood related disasters on treatment management, care and exacerbations of non-communicable diseases and the implications for public health. *PLOS Currents Disasters*. Edition 1, September 28.
- Schneider, H. 1998. "Close Call Spurs Disaster Plan Review." *The Washington Post*, January 25.
- Scott, R.D. 2006. *Ship to Shore Power: US Navy Humanitarian Relief?* [https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-691-seminar-in-electric-power-systems-spring-2006/projects/ship\\_to\\_shore.pdf](https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-691-seminar-in-electric-power-systems-spring-2006/projects/ship_to_shore.pdf).
- Singh, V. 2001. Blending wind and solar into the diesel generator market. *Renewable Energy Policy Project* 12.
- Sullivan, M., J. Schellenberg, and M. Blundell. 2015. *Updated Value of Service Reliability Estimates for Electric Utility Customers in the United States*. LBNL-6941E. <https://emp.lbl.gov/sites/all/files/lbnl-6941e.pdf>.
- The Economist. 1998. "After the storm, the clearing-up," January 15. <http://www.economist.com/node/110924>. Accessed July 11, 2017.
- The Ottawa Citizen. 2016. "Remember The Ice Storm of '98? It Was the Most Devastating and Least Ferocious of Canadian Disasters," February 24. <http://ottawacitizen.com/news/local-news/remember-the-ice-storm-of-98-it-was-the-most-devastating-and-least-ferocious-of-disasters>. Accessed July 11, 2017.
- Vertiv. 2016. "Benchmark Series." <https://www.vertivco.com/en-us/insights/articles/pr-campaigns-reports/benchmark-series/>. Accessed July 11, 2017.

# 6

## Restoring Grid Function After a Major Disruption

### INTRODUCTION

This chapter discusses the post-event system restoration and the learning phases of the resilience model laid out in Figure 1.2. The committee first introduces a general model for electricity system restoration after a large-area, long-duration outage and then discusses restoration for several classes of disruptions based on the type of damage caused. This organization is based on the recognition that restoration activities proceed differently based on different types of outages—following some events, utility operators will have no situational awareness to guide their deployments; whereas other events may leave monitoring systems intact but overwhelm stockpiled resources. The chapter includes recommendations for improving the restoration process and for improving post-incident investigation to better learn from each experience to improve future performance.

### GENERAL MODEL FOR ELECTRICITY RESTORATION

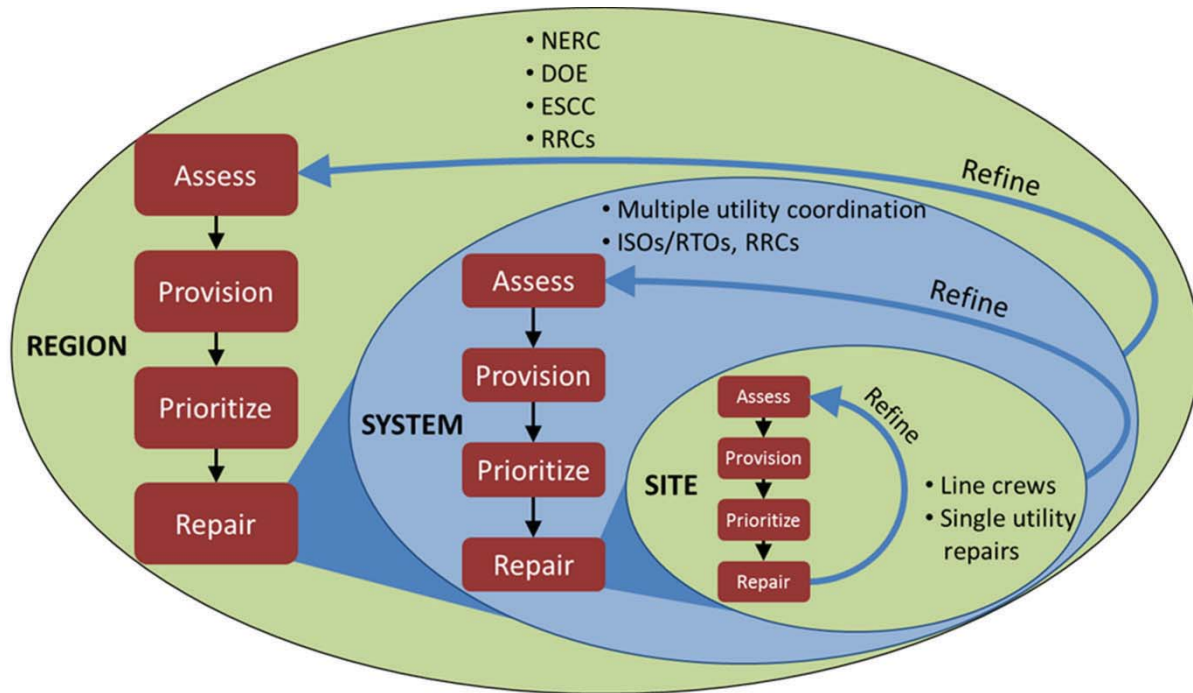
Following a large-area, long-duration outage, electricity system operators set priorities and work across organizational boundaries to bring the system back online as quickly as possible through a series of restoration activities. While the exact steps and procedures for restoration vary depending on the nature of the outage and the damage incurred, electricity providers follow four general restoration steps:

1. Assess the extent, locations, and severity of damage to the electricity system;
2. Provide the physical and human resources required for repairs;
3. Prioritize sites/components for repair based on factors including the criticality of the load and the availability of resources to complete the needed repairs; and
4. Implement the needed repairs and reassess system state.

As shown in Figure 6.1, these general processes are carried out simultaneously by different organizations operating

at different scales across all elements of the power system. Many of these organizations have their own restoration plans, spanning those from individual distribution cooperatives such as Cuivre River Electric Cooperative in Missouri (CREC, 2016), to large investor-owned utilities such as New York State Electric and Gas Corporation and Rochester Gas and Electric Corporation (NYSEG and RGEC, 2016), to independent system operators such as PJM (2016). Organizations frequently involved in electricity restoration include not only electricity system operators (i.e., distribution, transmission, and generation utilities and independent system operators), but also emergency management officials from city, county, state, and federal organizations, including the Federal Emergency Management Agency (FEMA), the Department of Energy (DOE), state emergency management agencies, the National Guard, and in some cases even the Department of Defense. Depending on the circumstances, organizations that operate far afield of the utility sector may be called on when they offer special capabilities—for example, the deployment of the U.S. Air Force to transport bucket trucks by air from California to New York in response to Superstorm Sandy. Effective restoration rests on the collaboration and cooperation of myriad organizations and individuals of different skills. Various mutual assistance agreements provide additional resources to extend the reach of the restoration across geographic and organizational boundaries. The restoration work itself is dependent on the skills and resources of the line and electrician crews deployed by the local utilities.

Coordination and communication among these groups is challenging, in part because each group has different responsibilities and boundaries within which it operates. Knowledge of local conditions and needs is greatest at the site level and diminishes with increasing scale, whereas understanding of systemic risks and critical needs may be greater at the regional scale. Thus, information must flow in both directions, and, while prior agreements can help considerably, communication channels specific to the actors and hazards involved are often established in an ad hoc manner.



**FIGURE 6.1** Illustration of the general processes of restoration that occur on multiple levels by different institutions with responsibility for electricity restoration.

NOTE: NERC, North American Electric Reliability Corporation; DOE, Department of Energy; ESCC, Electricity Subsector Coordinating Council; RRC, regional reliability coordinator; ISO, independent system operator; RTO, regional transmission organization.

These communications must be agile and flexible, evolving in response to changing conditions and the shifting composition of the restoration team. Communication is partly a technical issue and partly an organizational issue—for example, determining who should have access to information. In recent storms such as Superstorm Sandy, coordinating the dispatch and routing of crews through damaged and flooded areas was a challenge, and crews were sometimes delayed because they could not reach affected areas.

Beyond identifying a specific threat to the electricity system, key utility CEOs and federal decision makers meet through the Electricity Subsector Coordinating Council to plan for national-level incidents and maintain open communication channels (ESCC, 2016). This lays a good foundation for restoration activities, but an agile approach is necessary to deal with specific circumstances. Exercises are critical, although exercises alone will not address an actual event in all regards. Nonetheless, practice and associated learning will improve reactions during actual response.

During a major disaster, the states coordinate all first responder and restoration activities. For large incidents, when federal resources are warranted and mobilized, the National Response Framework provides the organizational structure, FEMA coordinates federal assets, and DOE is appointed the energy-sector lead agency (DHS, 2016). In preparation for or response to major outages, DOE will

staff local and headquarters operations centers to coordinate federal actions that expedite electricity system restoration, working closely with the electricity organizations involved and other responders. Examples of DOE action include waiving federal transportation regulations on the time trucks can drive continuously so as to bring necessary equipment to the affected area more rapidly.

When a physical disruption of the power system occurs, it is important that utility repair crews be able to gain rapid access to damaged substations and other facilities so they can safely isolate and de-energize hazardous components, retain and gain access to emergency communication equipment and supplies, promptly assess damage, and start the process of restoration. In that context, the issue of working with law enforcement to gain access becomes critical, both for reasons of safety and because supplying power can be a key component of disaster recovery and avoiding further risks and damages.

One possible strategy could be to designate selected utility personnel as “first responders.” While there have been efforts to move in this direction, they have become stalled because doing so could raise potential issues of liability, perhaps placing crews under state control or even requiring crews to divert their efforts away from electricity-related activities. The Edison Electric Institute (EEI) and others have been working at high levels to reach informal agreements

about achieving access. One problem with such an informal approach is that, without official credentialing, other first responders on the ground may not be aware of such arrangements and serious delays in access can occur. The situation could become even more complicated in the event of a major terrorist attack on substations or other critical grid facilities that might be designated as “crime scenes.” A similar situation could arise in the wake of a cyber attack where affected systems might be considered evidence.

**Finding:** When major physical damage occurs in the power grid, it is important that utility repair crews be able to gain rapid access. Due to a lack of standing arrangements with law enforcement and other first responders, this is not always possible; informal high-level agreements about access do not always result in smooth operations among key personnel on the ground.

**Recommendation 6.1:** The Department of Homeland Security in collaboration with the Department of Energy should redouble efforts to work with utilities and national, state, and local law enforcement to develop formal arrangements (such as designating selected utility personnel as “first responders”) that credential selected utility personnel to allow prompt utility access to damaged facilities across jurisdictional boundaries. Such agreements should address issues such as indemnity, liability, and the risk of diverting the mission and assets of utility crews to other non-power system objectives.

### Utility Planning for Restoration from Major Disruptions

Utilities are well practiced at recovering from localized damage to the grid and helping to restore the system outside their service areas following large events. From line crews to executives, utilities are familiar with recovery from regional natural hazards; they have developed restoration plans and allocated resources for recovery operations. Some utilities equip bucket trucks with mobile generators and communications equipment that allow line crews to maintain contact and proceed with repairs even when the bulk grid and communications infrastructures are down. When damages to the physical system exceed the hardware or human resources of a single utility, mutual assistance agreements (MAAs) are used widely throughout the industry to expedite sharing of crews and equipment among utilities. For larger events, crews and equipment are often brought in from thousands of miles away to aid restoration efforts in affected areas. Following Superstorm Sandy, the EEI developed a National Response Event framework for coordinating regional MAAs across the United States (EEI, 2016). Although the National Response Event framework has not yet been tested, it is designed to help prioritize and expedite dispatch of line crews and resources on a national scale with a comprehensive understanding of damages and restoration efforts.

Utility restoration plans emphasize advanced planning, communication, training, and continual refinement and improvement. Restoration plans are drilled by utilities and externally reviewed by the North American Electric Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC), and regional reliability organizations. One recent voluntary review found that participating organizations maintained system restoration plans that were thorough and highly detailed; however, opportunities for improvement remain (NERC, 2016a). For example, restoration plans may make key assumptions about the availability of certain assets (e.g., that a pre-identified black-start transmission corridor is operational) that, depending on the extent of damage, may not hold true.

Depending on the hazard, it may be possible for utilities to strategically deploy assets and for state and federal agencies to be mobilized in advance of the event. For example, utilities operating along the Gulf Coast have a long history of anticipating and recovering from large storms that cause extensive damage, and their restoration plans and activities reflect this history. In the week before Hurricane Katrina, Southern Company and its operating subsidiaries in Mississippi and Alabama spent more than \$7 million pre-staging personnel and supplies, including catering and amenities for restoration workers, many of whose families were directly impacted by the storm (Ball, 2006). The arrival of Superstorm Sandy was preceded by a large mobilization of assets by utilities and the federal government (Fugate, 2012; Lacey, 2014). Vermont Electric Power Company's Weather Analytics Center provides highly accurate weather forecasts that the utility uses to pre-position restoration crews and assets (NASEM, 2016). Developing additional technologies and strategies to improve pre-positioning of restoration assets remains an important area for additional effort.

The process of electricity system restoration begins long before a specific event or threat is identified, through extensive planning, training, drilling, and pre-positioning of assets, and continues after all service has been restored, through continual refinement of a utility's restoration plans. Fundamental to all restoration planning is an unresolvable uncertainty: the exact nature of damage cannot be known before an event occurs, and restoration plans must simultaneously be specific and actionable for utility personnel yet general enough to accommodate diverse potential scenarios. Thus there is no uniform, repeatable process for restoration that extends beyond a single event. There are many post-action reports from major outages that describe the event, how it was addressed by whom, and lessons learned. By systematically evaluating previous experiences and more openly sharing information about recovery from major outages, utilities have an opportunity to identify and share best practices. While such analysis is conducted on behalf of transmission utilities at the North American Transmission Forum, these assessments do not cover distribution utilities.



**Recommendation 6.2:** With support and encouragement from relevant state and federal regulatory agencies, the Department of Energy and utilities should continue to work together to analyze past large-area, long-duration outages to identify common elements and processes for system restoration and define best practices that can be shared broadly throughout the electricity industry. The committee notes that progress has been made with the ongoing efforts of the Electricity Subsector Coordinating Council, which provides a good framework for expanded coordination and sharing of best practices.

### Black-Start Recovery Plans

Large generation and transmission operators maintain restoration and recovery plans for energizing the high-voltage transmission system following a large-area, long-duration outage. Most generation facilities require electricity for operation, so if generators have gone off-line, these plans begin by starting selected “black-start” generators that do not require power from the larger grid to function. There are almost always functioning areas of the grid adjacent to the area experiencing an outage, and service can be most effectively restored from the edges of the blacked-out areas. If this is not the case, then black-start generators must first supply power to nuclear plants for safe shutdown before providing power to other generating stations. While black-start plans are difficult or impossible to practice (because doing so would require shutting down the grid), restoration plans provide detailed information on black-start resources in a utility’s service area, identify the priority loads and transmission corridors that the utility will bring power to first, and provide operators with key contact information. The priority loads for restoring the electricity system are other non-black-start generation plants—particularly nuclear plants that require external power—as well as natural gas pumping stations that maintain pressure in pipelines and provide fuel for natural gas generators to come online.

As generators and transmission corridors become energized, power is provided to distribution circuits—with priority given to known critical loads such as hospitals and repairs that restore service to the most customers. As restoration progresses, more generators are connected and resynchronized until service is restored to more loads. In some cases, this restoration may involve forming “islands” of electrical service: multiple smaller regions maintain balance of generation and load independent of the remaining grid and are then subsequently synchronized to the remaining system (PJM, 2016). Depending on how quickly generators are restored, some low-priority loads may need to remain off-line as the electricity providers will ration available supply to meet prioritized demand requirements. The time required to complete this process depends significantly on the damage to the infrastructure, the amount of data and information available, and the availability of restoration resources.

The Electric Power Research Institute (EPRI) has developed generic restoration milestones as well as a comprehensive

methodology for power system restoration based on these milestones. It is also developing and demonstrating a prototype decision support tool for evaluating system restoration strategies (EPRI, 2010). The Optimal Black-Start Capability tool can be used by utilities to evaluate the suitability of available black-start capable units and plan optimal locations and capacity levels for new black-start units.

The restoration process is highly dependent on the topology of the transmission and distribution networks, which determine the sequence of restoration starting from the black-start generators. If in the future the generation resources are more decentralized and placed on the distribution feeders, the topology of the grid, and hence the restoration process, becomes more complex. However, the smaller generation resources closer to the loads can make the generation-load balance easier during restoration, provided that these generators (and even responsive loads) have adequate controllability. With the higher penetrations of distributed energy resources (DERs), the restoration process will need to be rethought.

### Opportunities to Include Distributed Energy Resources in Restoration and Black Start

Traditionally, black-start plans have focused entirely on large, centralized utility generation assets. As the grid evolves to include larger amounts of DERs more broadly, it becomes important to consider the role these resources might play in the context of black start. The benefits and impacts of DERs will vary by geographic region because some distribution utilities have a higher penetration of DER assets than other areas. Additionally, some distributed generation and other assets are monitored and controlled by third-party entities other than the utility or grid operator because state policies do not allow these utilities to operate behind the meter. At low levels of penetration, DERs should simply be operated in ways that do not interfere with any needed black-start operations. As noted in Chapter 5, with appropriate system upgrades and institutional arrangements, microgrids and DERs could provide islands of power during outages; they could also provide local generation for utilities to restore from the distribution system outwards by connecting such small islands, as opposed to bringing power in from the bulk power system. While it may be possible to configure such resources to speed the process of supplying power to some priority loads, that would also unburden the primary black-start restoration process. At high levels of penetration, there may be an opportunity to factor DERs into black-start restoration plans. For example, multiple islands in the system formed by microgrids could be connected to form larger islands. Doing that might give the utilities more assets and more flexibility in their black-start planning.

**Finding:** The presence of a significant amount of DERs could provide a limited amount of local power during outages and could also be factored into black-start and



emergency planning if appropriate system upgrades have been made and utility operators have visibility into their operating status and controllability of their performance.

**Recommendation 6.3:** The Department of Energy and utilities should evaluate the technical and contractual requirements for using distributed energy resources as part of restoration activities, even when these assets are not owned by the utility, to improve restoration and overall resilience. Emergency management and restoration plans should include the owners of distributed energy resource assets, including owners with generation, storage, or load-control capabilities.

### Monitoring and Control

The monitoring and control of the power grid is accomplished through the supervisory control and data acquisition (SCADA) system and other supporting technologies, as described in previous chapters. At the control center, software tools aggregate diverse data to provide situational awareness and support operator decision making (e.g., energy management systems [EMS] on the transmission system and distribution management systems [DMS] on the distribution side). These systems gather measurement data from sensors deployed throughout the transmission and distribution systems and send out control signals. Additional sensor technologies exist for monitoring the health of circuits and components during and after restoration, which can confirm to repair crews that damage has been corrected; however, to the committee's knowledge, these have not been licensed or developed as commercial products. SCADA systems utilize robust, low-latency communications and are extremely helpful in assessing the state of damage to the system and identifying the centralized and distributed resources available for restoration. The communication networks enabling this monitoring and control are often dedicated infrastructure under the direct jurisdiction of the operating entity but are sometimes leased or provisioned by third parties.

DERs could also be monitored and controlled using the same SCADA system, in which case it would be easier for the DER to assist with restoration activities. If the DER is dispatched through a different monitoring and control communications infrastructure, it may be more difficult to provide restoration services due to the complications of coordinating among different systems. After a major disturbance, the status of the DERs, as well as the rest of the grid components, can only be known if the sensors and communication networks are not damaged or shut down by the disturbance. Electric power operators must restore power control systems and supporting communications systems concurrently with, and as an integral part of, grid restoration. Restoration of control systems and their associated communications infrastructure must remain an integral part of resilience planning.

### Recovery Depends on the Type of Damage

Beyond the generalized description of the recovery process, the details of restoration activities can be very different for different types of events and resulting damage. For example, a cascading blackout can cause a large area to lose power, but recovery may be relatively rapid and straightforward if no significant physical damage has been done to system components. Likewise, restoration—and specifically damage assessment—is considerably easier when the grid's cyber monitoring and control systems are intact and operational, compared to a potential cyber attack that diminishes a utility's situational awareness. In contrast, a strong, slow-moving hurricane can cause destruction and flooding over hundreds of square miles of coastal community, making post-event access very difficult. The following sections describe opportunities to improve recovery to outages with different types of damage, as categorized in Figure 3.2.

### DISRUPTIONS THAT INVOLVE ACROSS-THE-BOARD DAMAGE TO THE GRID AND ITS SUPPORTING INFRASTRUCTURE

Perhaps the most difficult disruptions to recover from are those that simultaneously cause damage to the physical components of the electricity system, the cyber monitoring and control systems, and critical supporting infrastructure. Damages of this sort can result from major natural disasters such as hurricanes and tropical storms, floods, winter storms, and earthquakes. Table 6A.1 provides details for each of these hazards in terms of the six stages of the outage life cycle—plan, prepare, event, assess, restore, and recover. Table 6A.2 lists two additional events, tornado and geomagnetic disturbances (space weather), that can also cause widespread damage.

While all of these events involve physical damage to the power system, there can be considerable variation in the extent of damage to other supporting infrastructures and the community. For example, damage from a major hurricane is typically widespread, inflicted on transportation and other critical infrastructures, and can greatly diminish local electricity consumption. In contrast, as Table 6A.1 notes, the spatial extent of damage from flooding depends significantly on local topology: in some cases much of the community may be unaffected, whereas communities and infrastructure in flat and low-lying terrains may be entirely destroyed. Clearly these two situations result in dramatically different restoration environments. Restoring a system from nearby dry ground that has all facilities intact and working is far easier than operating in an environment where everything for miles around has been submerged. Utilities generally know what sort of circumstance they will face in the event of a disaster and plan accordingly.

In some situations, there is sufficient warning time to assess whether critical system components will be at risk and, when possible, take preventative actions. While utilities

strive to maintain electrical service at all times, sometimes taking steps that will speed recovery after an inevitable outage should take precedence over keeping power on as long as possible before an outage. For example, a utility will know which substations are exposed to high flood risk and may preemptively power down certain parts of the system to prevent more substantial damage from flooding energized facilities. There are circumstances in which de-energizing vulnerable components *before* an event occurs could better protect them from damage and make recovery much faster.

**Recommendation 6.4:** Electric service providers should identify those components and corresponding events for which pre-event de-energizing of selected assets is the lowest risk strategy and develop regulatory, communication (especially with customers), and other plans that allow such protective action to be implemented.

### Assessing System Damage

As Figure 6.1 notes, the first step in restoration is to assess the state of the system. Where the monitoring and control system is still operating, it can be used to perform a rapid assessment. More monitoring and control is available at the transmission level, but SCADA at the distribution level is also being deployed, driven in part by the increase in DERs and other advanced technologies. This monitoring is also extending to the customer level with advanced metering infrastructure (AMI) and distribution technologies. Rather than depending on customer phone calls, some outage management systems (OMSs) receive direct telemetry from AMI and other sensors to develop a comprehensive view of customer outages.

Where the communications network supporting the SCADA system or other measurement telemetry is damaged, the traditional strategy is to send crews out to do on-site inspections. At the transmission level, aircraft are often used to locate downed lines, towers, and other damage. Normally aircraft would be operating directly under the jurisdiction of the electricity utility operator, as their assets are also used for routine right-of-way patrols. If necessary, electricity operators are able to acquire additional aircraft through leasing or other arrangements. During large national-level events, other government agencies can provide aerial surveillance capabilities if they are not directly involved in search and rescue operations. The Civil Air Patrol,<sup>1</sup> a civilian auxiliary

of the U.S. Air Force, has also been leveraged to provide aerial photographic sorties following disasters.

A new option coming into serious consideration is the use of unmanned aerial vehicles (UAVs), commonly known as drones (Olearczyk, 2013; Miller et al., 2014). Such vehicles can systematically survey damage to a system using both visible light and infrared imagery. Some UAVs have a fixed-wing design, but others are more maneuverable and can hover over problem areas for a long duration. The results of UAV inspections will be most useful if a utility has previously built a geocoded baseline of its entire system. This allows new imagery to be compared with baseline imagery and combined with asset management tools and workforce management systems to establish and coordinate repair priorities and progress (Miller et al., 2014).

The operation of UAVs in the United States is under the jurisdiction of the Federal Aviation Administration (FAA), which has been adopting new rules governing the commercial application of UAVs. However, these regulations have not kept pace with the rapid technological advancement of these systems, and there remains uncertainty surrounding the viability of UAVs for this application. In July 2016, Congress passed the FAA Extension, Safety, and Security Act of 2016.<sup>2</sup> Section 2207 of that law requires FAA, no later than 90 days after enactment, to “publish guidance for application for, and procedures for the processing of, on an emergency basis, exemptions or certificates of authorization or waiver for the use of unmanned aerial systems by civil or public operators in response to a catastrophe, disaster, or other emergency to facilitate emergency response operations, such as firefighting, search and rescue and utility and infrastructure restoration efforts.” As of this writing, that guidance has not yet been issued. A system that relies on temporary FAA authorization creates barriers to adopting this technology for electricity service restoration, since the capability to use UAVs for damage assessment needs to be developed, exercised, and refined in advance of a disaster rather than cultivated during the incident.

A continuing problem with the use of UAVs, both for post-disaster assessment as well as for routine surveillance and maintenance of transmission and distribution systems, has been the FAA restriction that such vehicles can only be used within the UAV pilot’s line of sight. In the event of a large-scale disaster, such a restriction seriously limits how useful UAVs can be. Several utilities have been experimenting with the use of UAVs and have obtained FAA 333 permits.<sup>3</sup> Some limited use of UAVs for post-disaster surveillance has also

<sup>1</sup> The Civil Air Patrol (CAP) is a congressionally chartered, federally supported non-profit corporation that serves as the official civilian auxiliary of the U.S. Air Force. CAP is a volunteer organization that performs three congressionally assigned key missions: emergency services (e.g., search and rescue and disaster relief operations), aerospace education for youth and the general public, and cadet programs for teenage youth. In addition, CAP has recently been tasked with homeland security and courier service missions. CAP also performs non-auxiliary missions for various governmental and private agencies, such as local law enforcement and the American Red Cross.

<sup>2</sup> Public Law No. 114-190 (2016).

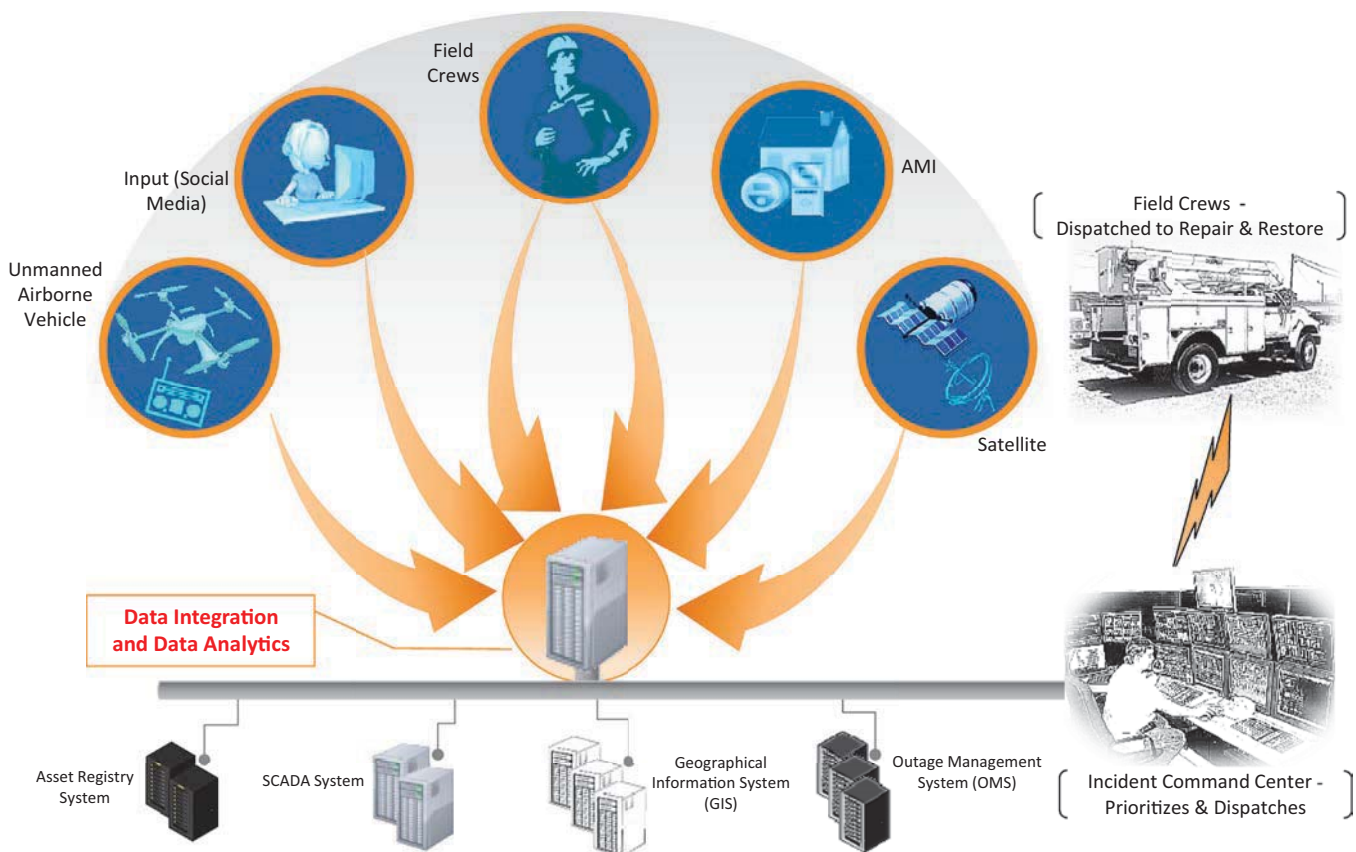
<sup>3</sup> FAA Section 333 “grants the Secretary of Transportation the authority to determine whether an airworthiness certificate is required for a unmanned aircraft system to operate safely in the National Airspace System.” As of 2015, the number of FAA 333 exemption permits granted to Duke was 16; San Diego Gas & Electric was 8; Pacific Gas & Electric was 5; Southern Company was 4; and NextEra Energy was 4.

occurred under FAA Part 107 waivers following Hurricane Matthew, which aided in damage assessment and expedited recovery. However, both Section 333 and Part 107 permits require pilots to maintain line-of-sight operations, and any operation beyond line of sight requires additional FAA authorization. At the time of this writing, very few waivers for granting operation beyond line of sight have been granted, and these have been primarily to specialized testing and research organizations. While FAA can grant exceptions on an ad hoc basis, this takes time. It would be far better to have standing arrangements for the use of drones in emergency situations.

**Recommendation 6.5:** With convening support by the Department of Energy, the electricity industry should proactively engage the Federal Aviation Administration to ensure that the rules regulating unmanned aerial vehicle operation support the rapid, safe, and effective applications of unmanned aerial vehicle technology in electricity restoration activities, including pre-disaster tests and drills.

### Data Fusion to Enhance Restoration Activities

In addition to the OMS that tracks customer outages and correlates these data with geospatial feeder data to determine where repair crews should be sent, other available data from various sources such as weather forecasts and news reports are being used to aid restoration activities (Figure 6.2). An area for research is the use of additional, underutilized information such as social media—Internet resources and social media are widely used to distribute information to consumers during a disaster. It is also possible to make use of information from consumers; however, systems are not generally in place to accomplish this. For example, during and immediately after Superstorm Sandy, many individuals sent images of downed lines, trees, and damaged equipment to utilities. If this information were automatically geotagged and time stamped, it could have provided valuable information to aid in restoration activities. Unfortunately, at the time, utilities struggled to make use of the information as it arrived in high volumes over non-traditional channels. Additionally, there was a need to ensure that public messaging was consistent,



**FIGURE 6.2** Example of data integration to support advanced data analytics for improved restoration efforts. The image above is not comprehensive and other technologies—for example, real-time asset health monitoring equipment and manned airborne vehicles—can be used to collect and relay information on the health of transmission and distribution system components.

NOTE: AMI, advanced metering infrastructure.

SOURCE: EPRI (2013).



such as continuing to advise the public never to approach downed electrical equipment.

### Access to Replacement Parts, Particularly Large Transformers

While line crews are able to repair downed power lines, towers, and poles, and repair or replace low- and medium-voltage distribution transformers, damage to large substation equipment can be much more problematic. These substations contain high-voltage transformers, circuit breakers, and other large equipment that, if damaged, can be difficult and expensive to replace. Extra-high-voltage transformers (i.e., 345 kV and above) are especially problematic. These are large devices that are expensive, have long manufacturing lead times, and are hard to move. In many cases, the electrical properties of high-voltage transformers have been customized to fit the specific locations in which they are installed. It has long been understood that these transformers are an especially vulnerable element of the grid (OTA, 1990; NRC, 2012; DOE, 2015; Parfomak, 2014). While spare transformers can become a major issue in outage events that cause broad physical damage, they are especially important in the context of terrorist events where they could become the focal target of intentional attack. Indeed, as far back as 1990, the Office of Technology Assessment concluded that, if a terrorist group wanted to attack the U.S. power system, the obvious target would be a carefully selected set of high-voltage power transformers. *Terrorism and the Electric Power Delivery System* explained the following:

The large power transformers in generating station switch yards and major substations are vulnerable to terrorist attack

and could take months or years to replace. Options for bypassing damaged substations to bring power from remote generating stations to load centers are very limited because the grid is already stressed during peak demand. The result of a coordinated attack on key substations could be rolling blackouts over a wide area until the substations are repaired. Under such conditions, the availability of compact easily transported recovery transformers would be invaluable (NRC, 2012).

The report went on to recommend that the Department of Homeland Security (DHS) cooperate with DOE to “complete the development and demonstration of high-voltage recovery transformers and develop plans for manufacturer storage and installation of these recovery transformers” (NRC, 2012). In a demonstration program called RecX (for “recovery transformer”), the DHS Science and Technology Directorate teamed with ABB and the power industry to manufacture three single-phase 345 kV transformers in St. Louis, Missouri, and move them to Houston, Texas, in March 2013 (Figure 6.3), where they were installed and operated in a substation. The entire move and installation was completed in less than 1 week (DHS, 2014).

Regulators, policy makers, and utilities recognize the need to stockpile spare equipment, especially large equipment that can be difficult and expensive to replace. As summarized in a recent Congressional Research Service report (Parfomak, 2014), the industry has made some progress in constructing a catalogue of spare high-voltage transformers. DOE recently released a request for information to gather input on setting up a national transformer reserve, and eight private energy companies have launched Grid Assurance,<sup>TM</sup> an independent company that will stockpile transformers



**FIGURE 6.3** Three ABB single-phase 345 kV compact replacement transformers being moved from St. Louis, Missouri, to a substation in Houston, Texas, under a Department of Homeland Security demonstration project.  
SOURCE: DHS (2012).

and other critical equipment.<sup>4</sup> A central issue with respect to developing a stockpile of replacement transformers is how to cover the cost. The approach taken by Grid Assurance,<sup>TM</sup> in which participating utilities have helped finance the founding of the company, and in return the company will sell stockpiled equipment to participating utility companies who need them during emergencies, was recently given a boost when FERC allowed participating utilities to recover their costs associated with purchasing sparing service and spare equipment.

Given the inherent challenge to knowing in advance where the need might arise to replace multiple transformers, some argue that building a modest stockpile is a collective national asset that should be covered, or at least partly subsidized, with federal tax dollars. Congress is contemplating the creation of a national strategic transformer reserve (DOE, 2017). However, if federal resources are invested in building such a stockpile, clear policy must be developed to limit its use to well-specified disaster scenarios. Without such policy, there is a risk that industry could become overly reliant on the stockpiled equipment and reduce investment in its own spare equipment stockpiles and programs. Such an outcome could result in negligible net improvement of spare equipment capability for the nation, rather than just shifting from industry-purchased stockpiles to government-purchased stockpiles.

In its 2015 Quadrennial Energy Review (QER), DOE noted that “the use of smaller, less-efficient, temporary replacement transformers may be appropriate for emergency circumstances. In 2006, [EPRI] suggested building compact ‘restoration transformers’ that would fit on large cargo aircraft and trucks. Since then, DHS’s Recovery Transformer Program has developed and tested a flexible transformer that is transportable by truck [see Figure 6.3] and can be installed within several days of an incident. These technologies could help address logistical concerns with moving large transformers in the event of disruptions” (DOE, 2015). The QER concluded that high-voltage transformers “represent one of [the grid’s] most vulnerable components. Despite expanded efforts by industry and federal regulators, current programs to address the vulnerability may not be adequate to address the security and reliability concerns associated with simultaneous failures of multiple high-voltage transformers” (DOE, 2015). The 2017 QER also discusses this issue, noting the following:

There are currently three key industry-led, transformer-sharing programs in the United States—NERC’s Spare Equipment Database program, Edison Electric Institute’s Spare Transformer Equipment Program, and SpareConnect. Another program, Recovery Transformer, developed a rapidly deployable prototype transformer designed to replace the most common high-voltage transformers, which

DHS successfully funded in partnership with Electric Power Research Institute and completed in 2014. . . . As of December 2016, three additional programs—Grid Assurance, Wattstock, and Regional Equipment Sharing for Transmission Outage Restoration (commonly referred to as RESTORE)—are in development. . . . In December 2015, Congress directed DOE to develop a plan to establish a strategic transformer reserve in consultation with various industry stakeholders in the FAST Act. To assess plan options, DOE commissioned Oak Ridge National Laboratory to perform a technical analysis that would provide data necessary to evaluate the need for and feasibility of a strategic transformer reserve. The objective of the study was to determine if, after a severe event, extensive damage to [large power transformers] and lack of adequate replacement LPTs would render the grid dysfunctional for an extended period (several months to years) until replacement LPTs could be manufactured. DOE’s recommendations will be published in the report to Congress in early 2017 (DOE, 2017).

Over the next two decades, the grid will see increasing use of solid-state transformers and other solid-state power electronics, though penetration at present is nascent. The durability and resilience of this technology will have to be established over time and restoration plans adjusted accordingly. Solid-state power electronics will offer greater operational flexibility than traditional technology, which may be useful when the grid is being operated in non-standard ways. This technology will likely see its first widespread use in lower-power distribution systems. Recently, DOE has been supporting the development of advanced designs for LPTs. Specifically, they have been working to do the following:

Stimulate innovative designs that promote greater standardization (i.e., commoditize LPTs) to increase grid resilience (i.e., faster recovery) in the event of the loss of one or more LPTs. To this end, new designs must maintain high efficiencies, have variable impedances, accommodate various high-side and low-side voltages, and be cost-effective compared to traditional LPTs. Projects would be expected to involve modeling, analyses, and exploratory research to assess the performance and economics of proposed designs (DOE, 2016). A critical value of [this] research, beyond the development of advanced designs, is increased standardization of components improving agile allocation during disasters (DOE, 2016).

The committee recommends a dual strategy: On the one hand, the nation should push forward to improving the availability of conventional and replacement transformers for use in the event of physical disruption. At the same time, DOE should continue to explore advanced LPT designs that, in the longer term, could lower cost and improve the efficacy of emergency replacements. The vulnerability to grid operation posed by accidental or intentional damage to high-voltage transformers has been understood for decades. While limited progress has been made to reduce this vulnerability, it continues to pose a serious risk to the power system.

<sup>4</sup> Grid Assurance<sup>TM</sup> ([www.gridassurance.com](http://www.gridassurance.com)) was founded by affiliates of American Electric Power, Berkshire Hathaway Energy, Edison International, Eversource Energy, and Great Plains Energy.



## RESTORING GRID FUNCTION AFTER A MAJOR DISRUPTION

**Recommendation 6.6:** The Department of Homeland Security, the Department of Energy, the U.S. Congress, and the power industry should be more aggressive in finding a way to address the issue of manufacturing and stockpiling flexible, high-voltage replacement transformers as an important component of infrastructure investment initiatives. If federal funds are used to help in doing this, policy will be needed to limit stockpile use to major disasters. Otherwise, utilities might face incentives to reduce their stockpiles for dealing with more routine events.

**Finding:** Development of innovative approaches for making LPTs with greater operational flexibility (e.g., variable impedances, accommodating multiple voltages) while maintaining high efficiency and cost effectiveness relative to traditional LPTs is promising. If such devices can be developed with standardized components, they could play an important role in expediting restoration of the grid when physical damage has occurred to LPTs.

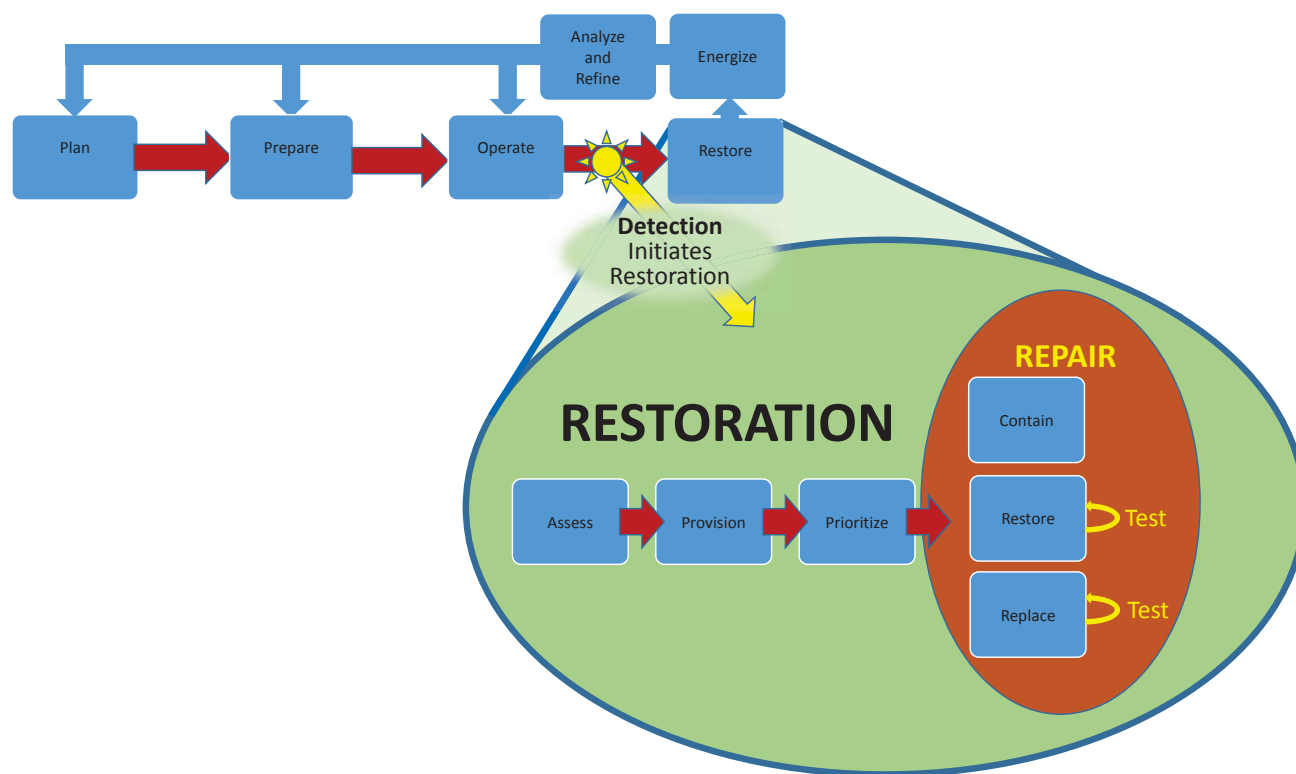
**Recommendation 6.7:** The Department of Energy should continue to support research and development of advanced large power transformers, concentrating on moving beyond design studies to conduct several demonstration projects.

## DISRUPTIONS THAT INVOLVE DAMAGE TO THE CYBER MONITORING AND CONTROL SYSTEMS

A second restoration case is recovery from damage to the cyber monitoring and control system as a result of a cyber attack that leads to a major service disruption. Restoration from such disruptions is structured around the process shown in Figure 6.4, which contextualizes active restoration within the larger process that begins with planning for cyber restoration in much the same way as utilities plan for physical restoration. Active cyber restoration begins with detecting a breach and follows the same sequence of activities introduced above: assess, provide, prioritize, and repair. This section focuses on the steps that occur to restore power after a cyber detection that has resulted in a major service disruption.

## Detect

One important difference between a cyber failure and a physical disaster is the tightly defined nature of the cyber attack. The impact of a hurricane is expressed in maps as well as in lists of damaged equipment and lines. In the case of a cyber event, the cause is usually more singular than that of a natural disaster. It would be a rare event that would involve the simultaneous breach by two disparate organizations in two different ways, although a well-prepared mal-actor



**FIGURE 6.4** Restoration of industrial control systems after a cyber breach.

may seek to create exactly this situation. The analysis of a cyber event typically focuses on understanding a specific bit of malware and how it affects communication, and the countermeasures are similarly focused and technical unless the impact extends to the point of requiring replacement of substantial equipment.

A breach of a utility industrial control system (ICS) can be obvious after the system it is controlling malfunctions, but this malfunction may not occur for a long time after the initial breach. For example, in the well-covered breach of the Ukrainian power system, the actual disruption occurred 9 months after the initial breach. Mandiant (2016) reported that the average time from breach to detection in a typical information technology system is 140 days. This time delay is important and pernicious as it allows attackers to locate and master critical systems, find valuable or restricted information, and develop a strategy for exploitation. Adversaries lacking detailed knowledge of a system do not know a priori how to inflict damage even if they have accessed the ICS; they need this time to learn how to damage the breached system. The first step in cyber restoration is to detect the breach quickly, so that the adversary does not have time to develop sufficient understanding of the ICS to disrupt operations. Utilities need to develop reliable mechanisms to verify that their systems are running only the expected software and, if this is not the case, to allow remote resetting of systems.

**Finding:** Breaches of utility industrial control systems may persist for an extended period prior to causing disruptions to operations or service. A breach alone is not sufficient to gain control of a system, to compromise its operation, or to steal or corrupt valuable information. It takes time for attackers to learn about the system they have breached.

The problem of breach detection can be addressed by anomaly detection, although this approach has not been shown to work as well in more general enterprise settings. In part, this is because complex and distributed systems of large enterprise systems are difficult to monitor, as the variety of communications is immense (e.g., from e-mail to web site configuration management and integration with multiple systems) and varies over time. However, electric utility ICS systems are different. The boundaries of the system are more clearly defined and slower to change, the network architecture is more consistent, the communications are more structured (i.e., using well-defined protocols), and the values communicated fall into definable ranges and patterns. For example, residential meters typically report every day, hour, or 15 minutes, depending on configuration; they always use a message structure defined by the brand of meter (frequently based on an open standard), and the voltages they report are almost always in the American National Standards Institute band.<sup>5</sup> Using another protocol,

reporting a value substantially outside the American National Standards Institute band, issuing a different message type, or reporting too often could indicate that the meter has been compromised or is malfunctioning. Another example of the potential for anomaly detection is reclosers, which control the connection to a lateral power line and do not open or close very often. Too-frequent cycling could indicate an attempt to damage the system.

Beyond these patterns, the electricity system is governed by the physics of its electrical flows. Information from the numerous and diverse sensors must present a coherent model of the state of the conditions on the grid. Reported values which deviate from the physically possible can indicate either a broken sensor or a cyber issue. For these reasons, anomaly detection methods that are not effective in general enterprise systems can work well in utility control systems. Anomalies can be detected based on rules derived by various means, including those that are (1) specified by operators, (2) derived from network mapping, (3) derived through machine learning, and (4) based on physical modeling. The first two of these are based on established technology (e.g., The Bro Project<sup>6</sup> and the Essence Project<sup>7</sup>). There is much potential for progress in the latter two. Machine learning could combine support vector machine estimation for classification with neural net methods for training. While good physics models are available (e.g., OpenDSS and GridLab-D for distribution systems), there are challenges in making them fast enough for use in real-time anomaly detection.

**Finding:** Tools for physics models and ICS network modeling are not well adapted to use in anomaly detection or cyber testing. Any discrepancy between the physics of the grid and the telemetry can indicate a system or component problem or a cyber compromise. The challenge at present is that physics models of power flow are generally too slow for real-time monitoring, and the track record for calibration is spotty.

**Recommendation 6.8:** The Department of Energy should develop the ability to apply physics-based modeling to anomaly detection. There is enormous value in having real-time or better physics models in deriving optimal power flow and monitoring performance for more accurate state estimation. Such systems should also provide a powerful tool for verifying the integrity of telemetry systems—that is, verifying that observed conditions are consistent with model conditions—and if not, then there is a problem with knowledge of state, presuming the model is accurate.

<sup>5</sup> American National Standards Institute Standard C84.1 defines the acceptable range of voltage within which a utility can deliver power to customers.

<sup>6</sup> The website for the Bro Project is <https://www.bro.org/>, accessed July 11, 2017.

<sup>7</sup> The website for the Essence Project is <https://www.controlsysteamsroadmap.net/Efforts/Pages/Essence.aspx>, accessed July 11, 2017.

## Assess

Once a breach of the ICS has been detected, the next step is to assess the extent of damage. At this point, power may still be flowing to part or all of the grid; however, the system has failed fundamentally because the ability to determine system state accurately and control component behavior is likely compromised. Work should begin immediately to determine what part of the system (including the ICS, all connected components, and communications in either direction with external systems) has been compromised and how. At the simplest level, this involves examination of all components for indicators of compromise. Examination can include the following:

- *Inspection.* Scanning the memory and storage of each device looking for malware (i.e., “blacklisting”) and checking that only approved software is running (i.e., “whitelisting”).
- *Challenge.* Exercising devices to verify that they are communicating and operating correctly (e.g., flip a switch electronically to verify that it can be reached, acts as directed, and can confirm its action and state).
- *Diagnostic model.* Network and physics-based modeling of the grid to map anomalous behavior, although currently the models that would be used for this are not yet ready to support near-real-time restoration.

The first steps in assessment are to assemble the necessary tools if they are not present, make sure that the tools and their underlying databases are up-to-date, and then systematically and completely examine every software object in the broadly defined system to determine whether and how each has been corrupted. The assessment should be undertaken with a sense of the system connectedness, first emphasizing components that are linked to and dependent on systems known to be compromised, within the same security domain, or accessed in similar ways.

## Provide

The provisioning phase of restoration focuses on marshalling human and other resources necessary to bring the ICS back to operation, perhaps in stages. Based on the assessment, the restoration team derives a list of skills and artifacts necessary to restore each component and the integrated system. In instances where replacement is either necessary or more efficient, these lists will include hardware (e.g., servers, smart components). For example, if a server is corrupted, it may be possible to restore it to safe operation, but it may be quicker and easier to build a new server from scratch and return the original server to inventory at a less hectic time. Restoration may also require software and data: reference disks of software, often termed “gold disks,” are typically required, as are backups of the most current

state data. Large transmission organizations are generally scrupulous about maintaining “gold disks,” but this practice has not been promulgated throughout the entire industry. Restoration can be slowed by something as simple as not having license information, not patching backups to current levels, or not having internet access when it is required for activation or download of current patches. The provisioning plan should take all of these activities into consideration. The provisioning plan, overlaid on the assessment, provides a map of what components and subsystems can be restored and with what effort.

## Prioritize

Based on the assessment, a plan must be developed to restore the system. The challenge is to coordinate the activities of specialists with the available physical and digital resources in a sequence of steps. Restoration of a specific computer could range from something as simple as running a virus removal tool to something as complex as writing new code for a virus removal tool. It could involve re-flashing a build image, replacing a drive or even a whole computer, or rebuilding a software configuration step-by-step. There may be hundreds of steps, and it may be impossible to determine in detail all of the steps needed in a particular case. Initially, the plan may state only that a network engineer will look at an infected switch and determine what needs to be done to repair it. As the restoration proceeds, knowledge of state and the efficacy of restoration options improve, and the plan becomes more specific.

A critical issue is the affected utility’s ability to marshal appropriately skilled resources. The design and documentation of utility ICS systems is insufficiently standardized; outside experts cannot quickly become effective in another organization. They can be tasked with routine tasks like imaging a disk, but their ability to contribute more strategically requires more detailed knowledge of affected systems. Priorities to achieve cyber resilience include establishing a common design and technical lexicon, training and working across organizations, and establishing common practices and formats for supporting artifacts. These need not be accomplished across the nation in a single push; rather, they can develop in groups of related or associated organizations, such as the group of distribution cooperatives supported by the single generation and transmission cooperative North Carolina Electric Membership Corporation. This model should be broadened to include other peer groups, perhaps organized around regional transmission organizations and regional reliability coordinators.

Another major barrier is that, to date, organizations have not been transparent about cyber events, in part owing to risk of embarrassment and liability. Furthermore, mechanisms to share resources for cyber restoration and compensate for their use—that is, cyber mutual assistance agreements analogous to traditional MAAs—are nascent. Working with

EEI, the Electricity Subsector Coordinating Council is developing such a cyber MAA program (ESCC, 2016); however, the configuration of local systems can differ so substantially across utilities (i.e., when comparing a small cooperative to a major independent system operator/regional transmission organization) that it may be prohibitively difficult for loaned workers to contribute significantly to cyber restoration, even if they are experts. Through a separate program, the Electricity Information Sharing and Analysis Center (E-ISAC) disseminates risk information to utilities; its further development should be encouraged, but the emphasis to date has been on sharing information rather than labor and primarily directed at protection rather than restoration.

One final issue to consider is funding; cyber restoration, like physical restoration, can be costly. Means must be made available for utilities to hire outside assistance when useful and buy new equipment as needed to restore power quickly. A utility may look at its limited resources and plan restoration over a long period, but there may be a social advantage to using resources beyond the utility to restore over a shorter period.

**Finding:** To date, there have been no large-scale power outages in the United States caused by cyber attacks, but there have been many instances in which components have been compromised. Utilities have experience in fixing these minor cyber problems by rebuilding components and databases. However, cyber restoration is not a routinized process, and different organizations follow different approaches based on the nature of the event.

**Recommendation 6.9:** The Department of Energy and the Department of Homeland Security should work with the North American Electric Reliability Corporation, independent system operators, and regional transmission organizations to develop a model for large-scale cyber restoration. This should be done in collaboration with utilities and leading utility organizations such as the Edison Electric Institute, the National Rural Electric Cooperative Association, the Electric Power Research Institute, and the American Public Power Association.

## Repair

Actual repairs are accomplished in three steps: (1) containing the breach, (2) restoring components that can be saved, and (3) replacing those that cannot.

## Contain

The first step after detection is to contain the malware by isolating it and preventing its spread to other internal or external systems. Taking an infected component off-line can adversely impact grid operations; thus, expert decisions must be made about how to operate without the impacted

components. Operations without compromised or degraded digital control may be possible; if not, a portion of the grid may be operated instead. For example, if the problem impacts voltage control at a particular substation, the feeder may be disconnected from central control and either operated with fixed typical control points or shut down temporarily. In this case, potentially no service will be lost. It is critical to keep safety and the long-term reliability of the grid in mind; operation should not be attempted unless it can be verified that the grid and customers are not put at risk. If digital telemetry is lacking, this may require dispatch of crews to verify switch settings manually, determine voltage and current, or confirm whether a line is energized. Fortunately, protective relays and fuses provide some protection against egregious misoperation.

Another aspect of containment is to communicate with other utilities. Sharing details of the attack—particularly information on the types of components impacted, the IP addresses of the attackers if known, and any identified malware signatures—may help others identify an ongoing attack. The E-ISAC has taken on the role of intermediary in this action; nonetheless, these systems must be strengthened, extended, accelerated, and exercised. The Cybersecurity Risk Information Sharing Program, initiated by DOE with E-ISAC support, is currently monitoring the majority of transmission systems and sharing such information with automated machine-to-machine communication. This has led to substantial improvement in the situational awareness of real-time cybersecurity risks in the electricity industry.

## Restore and Replace

With the spread of malware contained to the extent possible, the work shifts to restoring components to a clean state or replacing them if repair is too difficult or time consuming. As practice in cyber restoration moves beyond improvisation, restoration will eventually proceed by following a plan that is developed in advance, updated, and refined for specific circumstances. Implementing the plan requires the following: (1) Executing the outlined steps, (2) Adding detail as necessary and possible, (3) Testing, (4) Monitoring progress and failure, and (5) Providing feedback to update the plan.

At each point in the restoration, the engineer must determine the correct strategy: restore or replace. The trade-offs include cost, time, and the relative risk of a repaired component still hiding malware or being otherwise compromised versus possible errors in the configuration of new components. The choice is specific to the circumstances at hand. For example, the time required for repairs depends critically on whether there is a tested and trusted tool available on hand to remove malware and whether complete and correct backup data are available.

Highly competent staff are key to effective execution of restoration and replacement plans. While a utility may



have excellent general support staff, it is unlikely that they will have experience in large-scale cyber restoration. Their skills, experience, and confidence must allow them to innovate and improvise beyond their current skills. Government teams experienced in cyber restoration and similarly skilled staff from other utilities, software vendors, and cybersecurity firms can provide valuable support to the utility teams, although they are still limited by their lack of experience with the particular system being restored.

**Finding:** There has been a tendency among utilities and other commercial entities not to share information about cyber breaches and to look inward rather than seeking help, which limits potential for collaboration across organizations. Most utilities are not likely to have adequate internal staff directly experienced in large-scale cyber restoration. Furthermore, the ability of outside entities to help a utility with cyber restoration is limited by unfamiliarity with the configuration of the impacted system and by the lack of agreed-upon standards or shared practices. The ICS architecture at one utility may have little in common with the ICS at another utility, independent of the physical differences in the electrical system. This lack of commonality in utility ICS system designs and documentation makes rapid and efficient use of staff from other organizations very challenging, as an engineer at one utility may face a steep learning curve at another utility.

**Recommendation 6.10:** The Department of Energy and the Department of Homeland Security should work with the Electricity Subsector Coordinating Council and utilities to enhance the sharing of cyber restoration resources (i.e., cyber mutual assistance agreements) including personnel, focusing on peer-to-peer collaboration, as well as engagement with government, industry organizations, and commercial cybersecurity companies. Practices that allow shared personnel to more quickly come up to speed on restoration plans will increase the value of cyber mutual assistance agreements. This should include dissemination of best practices for the backup of utility industrial control systems and operational data.

**Finding:** Though the basic systems are in place for sharing cyber threat information, practices can be improved with more emphasis on speed. There are organizational systems in place for sharing cyber information (e.g., E-ISAC), but the lack of a common ontology and design patterns make the shared information more difficult than necessary to put to use.

**Recommendation 6.11:** The Department of Energy, the Department of Homeland Security, the electricity sector, and representatives of other key affected industries and sectors should continue to strengthen the bidirectional communication between federal cybersecurity programs and commercial software companies.

Effective documentation strategies are also critical for effective cyber restoration. System documentation must be complete, accurate, and up-to-date so that the restoration teams have the information they need to proceed and additional staff can be brought up to speed quickly. Industry experience has shown that the only way to keep documentation up-to-date is to connect it to operational production systems. For example, the network should be mapped periodically and continuously using automated tools, and then the discovered reality can be compared to the documented theory. Documentation should include backup copies of every critical system, including the data and software and all critical keys, passwords, and licenses. Such backup information should be available through a secure system with an expert in the loop.

Finally, cyber restoration workers need the best possible tools to facilitate their collaboration. At a minimum, telephones should be supplemented with shared drives, online screen sharing, and remote disk access. Cloud options should be available to provide backup if local systems are compromised to the extent possible and vice versa. Such cloud systems must be as secure as possible and potentially open only to utility operators. Furthermore, these teams must practice with either real systems or high-fidelity models. (It is possible to construct virtual systems that would allow training and practice.) Strategies for this sort of simulator are being pursued by DOE, with the National Renewable Energy Laboratory in the lead, and by the National Rural Electric Cooperative Association, with its Simba project.

## Energize

Restoration of the ICS culminates with energizing the grid, shown at the top of Figure 6.4. There needs to be rapid iteration and tight integration between the plan and test steps, but ultimately the real-world test in the grid cannot be achieved digitally and virtually. Utility ICSs have switches and other controls that set machines in motion and power flowing. Some of these actions can be dangerous to line crews and could cause damage to utility and customer equipment as well as to other infrastructures. Also, a compromised control system may incorrectly alter limits on a fault protection relay or send signals to a generator that crews on site in the plant know are incorrect, resulting in dangerous system operations.

The scale and importance of utility operations dictate validation in many aspects of cyber restoration. The physics of the grid must be considered in all cyber decisions. Expert judgment is needed to determine when physical contact and observation are needed and when the benefits outweigh the risks. The training of utility personnel ensures a culture of safety.

## Analyze and Refine

After the grid is re-energized, the final step is to examine what was accomplished and gather lessons learned. The goal

**TABLE 6.1** Summary of Selected Recommendations Made by the National Research Council in Its 2012 Report *Terrorism and the Electric Power Delivery System*, Together with the Committee's Assessment of Where Things Now Stand

National Research Council Recommendation	Assessment of Present Situation
<b>6.1:</b> The Electric Reliability Organization (ERO) [NERC] should require power companies to re-examine their critical substations to identify service vulnerabilities to terrorist attack. Where such vulnerabilities are discovered, physical and cyber protection should be applied. In addition, the design of these substations should be modified with the goal of making them more flexible to allow for efficient reconfiguration in the event of a malicious attack on the power system. The bus configurations in these substations could have a significant impact on maintaining reliability in the event of a malicious attack on the power system. Bus layout or configuration could be a significant factor if a transformer, circuit breaker, instrument transformer, or bus work is blown up, possibly damaging nearby equipment.	The industry has made progress on this issue.
<b>6.2:</b> The ERO and FERC should direct greater attention to vulnerability to multiple outages (e.g., n-2) planned by an intelligent adversary. In cases where major long-term outages are possible, reinforcements should be considered as long as costs are commensurate with the reduction of vulnerability and other possible benefits.	Some progress has been made on these issues, but additional effort is warranted.
<b>7.6:</b> State legislatures should change utility law to explicitly allow microgrids with distributed generation. [Institute of Electrical and Electronics Engineers] should revise its standards to include the appropriate use of islanded distributed generation and microgrid resources for local islanding in emergency recovery operations. Utilities should re-examine and, if necessary, revise their distribution automation plans and capabilities in light of the possible need to selectively serve critical loads during extended restoration efforts. Public utility commissions should consider the potential emergency restoration benefits of distribution automation when they review utility applications involving such investments.	There has been some progress on this. Some states are considering whether and, if so, how to support the development of microgrids as well as the role of the local distribution utilities and other entities in the process of developing such systems. But additional effort is warranted.
<b>8.1:</b> The Department of Homeland security and/or the Department of Energy should initiate and fund several model demonstration assessments each at the level of cities, counties, and states. These assessments should examine systematically the region's vulnerability to extended power outages and develop cost-effective strategies that can be adopted to reduce or, over time, eliminate such vulnerabilities. These model assessments should involve all relevant public and private participants including public and private parties providing law-enforcement: water, gas, sewage, healthcare, communications, transportation, fuel supply, banking, and food supply. These assessments should include a consideration of outages of long duration ( $\geq$ several weeks) and large geographic extent (over several states) since such outages could require a response different from those needed to deal with a shorter duration events (hours to a few days).	To the best of the committee's knowledge, no such demonstrations have been undertaken.
<b>8.2:</b> Building on the results of these model assessments, DHS should develop, test, and disseminate guidelines and tools to assist cities, counties, states, and regions to conduct their own assessments and develop plans to reduce their vulnerabilities to extended power outages. DHS should also develop guidance for individuals to help them understand steps they can take to better prepare for and reduce their vulnerability in the event of extended blackouts.	To the best of the committee's knowledge, no such activity has been undertaken.
<b>8.3:</b> State and local regions should use the tools provided by DHS as discussed in Recommendation 8.2 to undertake assessments of regional and local vulnerability to long-term outages, develop plans to collaboratively implement key strategies to reduce vulnerability, and assist private sector parties and individuals to identify steps they can take to reduce their vulnerabilities.	While not following the strategy that the committee recommended, some limited progress has been made.
<b>8.4, 8.5, and 8.6:</b> Congress, DHS, and the states should provide resources and incentives to cover incremental costs associated with private and public sector risk prevention and mitigation efforts to reduce the societal impact of an extended grid outage. Such incentives could include incremental funding for those aspects of systems that provide a public good but little private benefit, R&D support for new and emerging technology that will enhance the resiliency and restoration of the grid, and the development and implementation of building codes or ordinances that require alternate or backup sources of electric power for key facilities. . . . Federal and state agencies should identify legal barriers to data access, communications, and collaborative planning that could impede appropriate regional and local assessment and contingency planning for handling long-term outages. Political leaders of the jurisdictions involved should analyze the data security and privacy protection laws of their agencies with an eye to easing obstacles to collective planning and to facilitating smooth communication in a national or more localized emergency. . . . DHS should perform, or assist other federal agencies to perform, additional systematic assessment of the vulnerability of national infrastructure such as telecommunications and air traffic control in the face of extended and widespread loss of electric power, and then develop and implement strategies to reduce or eliminate vulnerabilities. Part of this work should include an assessment of the available surge capacity for large mobile generation sources. Such an assessment should include an examination of the feasibility of utilizing alternative sources of temporary power generation to meet emergency generation requirements (as identified by state, territorial, and local governments, the private sector, and nongovernmental organizations) in the event of a large-scale power outage of long duration. Such assessment should also include an examination of equipment availability, sources of power generation (mobile truck-mounted generators, naval and commercial ships, power barges, locomotives, and so on), transportation logistics, and system interconnection. When areas of potential shortages have been identified, plans should be developed and implemented to take corrective action and develop needed resource inventories, stockpiles, and mobilization plans.	Limited progress has been made on selected items.

National Research Council Recommendation	Assessment of Present Situation
<p><b>9.1:</b> Complete the development and demonstration of high-voltage recovery transformers and develop plans for the manufacture storage and installation of these recovery transformers.</p> <p><b>9.2–9.6:</b> Continue the development and demonstration of the advanced computational system currently funded by the Department of Homeland Security and underway at the Electric Power Research Institute. This system is intended to assist in supporting more rapid estimation of the state of the system and broader system analysis. . . . Develop a visualization system for transmission control centers which will support informed operator decision making and reduce vulnerability to human errors. R&amp;D to this end is underway at the Electric Power Research Institute, Department of Energy, Consortium for Electric Reliability Technology Solutions, and Power System Engineering Research Center, but improved integration of these efforts is required. . . . Develop dynamic systems technology in conjunction with response demonstrations now being outlined as part of an energy efficiency initiative being formed by EPRI, the Edison Electric Institute, and DOE. These systems would allow interactive control of consumer loads. . . . Develop multilayer control strategies that include capabilities to island and self-heal the power delivery system. This program should involve close cooperation with the electric power industry, building on work in the Wide Area Management System, the Wide Area Control System, and the Eastern Interconnection Phasor Project. . . . Develop improved energy storage that can be deployed as dispersed systems. The committee thinks that improved lithium-ion batteries have the greatest potential. The development of such batteries, which might become commercially viable through use in plug-in hybrid electric vehicles, should be accelerated.</p>	<p>A demonstration has been successfully conducted. Considerable work is still needed on developing and implementing an adequate program of funding and other support for recovery transformers.</p> <p>Limited progress has been made on selected items.</p>

NOTE: NRC (2012) was undertaken for the Department of Homeland Security. Progress has been limited on a number of the recommendations that are listed on page 6 of that report.  
SOURCE: NRC (2012).

is to refine the process, further moving cyber restoration from an ad hoc exercise to an engineering process.

**Recommendation 6.12:** The Department of Energy should develop a high-performance utility network simulator for use in cyber configuration and testing. There is, to date, no flexible, peta-scale utility industrial control system simulator that offers sufficient fidelity for testing intrusion detection, anomaly detection, software defined network controls, and other aspects of utility operations. The closest systems to date take a “hardware-in-the-loop” approach. While this offers some apparent advantages in terms of fidelity, it is too time consuming and expensive to test a wide range of scenarios in such a system. A purely virtual system is necessary.

**DISRUPTIONS THAT INVOLVE ONLY PHYSICAL DAMAGE**

There are few hazards that cause *only* physical damage to the electricity system. Of principal concern is the threat of a well-coordinated and executed physical attack. This was the subject of a 1990 Office of Technology Assessment report (OTA, 1990) and a more recent National Research Council report, *Terrorism and the Electric Power Delivery System* (NRC, 2012). While distribution and transmission equipment have been the target of attacks internationally, the Metcalf incident (described in Chapter 3) is one of the few cases in the United States, although the event was modest in scale and did not disrupt electricity service.

A terrorist attack on the towers and poles of the transmission infrastructure could disrupt service over a large area.

However, utilities are well practiced at rebuilding lines and replacing poles, and it is unlikely that such an outage would be of long duration. The situation is very different for an attack on substations and especially high-voltage transformers. As noted in *Terrorism and the Electric Power Delivery System*, a terrorist attack carried out in a carefully planned way by people who knew what they were doing could “deny large regions of the country access to bulk system power for weeks or even months. An event of this magnitude and duration could lead to turmoil, widespread public fear, and an image of helplessness that would play directly into the hands of the terrorists. If such large extended outages were to occur during times of extreme weather, *they could also result in hundreds or even thousands of deaths due to heat stress or extended exposure to extreme cold*” (NRC, 2012).

Table 6.1 revisits the recommendations made by that report and summarizes the present state of affairs. Unfortunately, the ubiquity of grid assets and their inherent vulnerability make it too costly to achieve a comprehensive high level of security. Resources are prioritized on those assets where improved security will yield the greatest improvement. Efforts to improve security at key assets should proceed alongside efforts to stockpile replacement equipment and develop and deploy temporary recovery assets.

**Finding:** The power system continues to be vulnerable to physical attack by terrorists. Some progress has been made in making the system more resilient in the face of this hazard—for example, through physical security standards such as NERC CIP-014—but much remains to be done. Several

strategies (e.g., high-voltage replacement transformers) that reduce vulnerability to terrorist events also reduce the system's vulnerability to a range of natural hazards.

**Recommendation 6.13:** Efforts by the Department of Energy and the Department of Homeland Security, in conjunction with the Federal Energy Regulatory Commission, the North American Electric Reliability Corporation, and the electric industry, should be redoubled to reduce the vulnerability of the power system to terrorist attacks (paying particular attention to topics in Table 6.1 that have not yet been adequately addressed).

## DISRUPTIONS THAT CAUSE BOTH PHYSICAL AND CYBER DAMAGE

Restoration of electric service from a system that has sustained both physical damage (e.g., a damaged transformer) and compromised monitoring and control systems (e.g., SCADA and EMS disrupted) will require greater reliance on manual inspection and operation, which can slow the pace of damage assessment and recovery. Thus, recovery from a coordinated cyber-physical attack may proceed slowly if operators suffer diminished situational awareness and have to dispatch linemen to assess damage. The principal concern across the industry is the potential for a well-informed state actor or terrorist group to execute a coordinated cyber-physical attack, the so-called structured adversary. Both cyber and physical attacks can be combined, targeted toward system components that cause the most damage or are most difficult to replace, and carried out repeatedly and perhaps with the explicit intent of hindering restoration.

EPRI has developed scenarios of coordinated cyber-physical attacks targeting generation, transmission, and distribution systems that can be used by operators and asset owners to test their readiness and improve planning and drilling (EPRI, 2012). More recently, NERC coordinated more than 100 participating organizations in the biennial distributed-play exercise GridEx III, which practiced response and recovery from a series of hypothetical cyber and physical attacks (NERC, 2016b). Such planning and drilling exercises are a valuable industry practice; however, the level of sophistication of attacks may continue to grow along with the number of vulnerable cyber and physical targets.

**Recommendation 6.14:** Utilities, with support from federal and state government, should continue to expand joint cyber-physical recovery exercises. These should emphasize, among other things, the maintenance of cyber protection during the chaotic period of physical restoration. The need to reconfigure electrical systems during a disaster requires changes to the industrial control system. It is frequently necessary to disable elements of the cybersecurity systems while the state of the grid is in flux. Research should be done on how to maintain a higher level of security during this period. This

may involve operation in default modes or with analog controls to some extent until cybersecurity can be reestablished.

## OPPORTUNITIES TO IMPROVE RESTORATION

### Other Technologies and Operations That Improve Restoration

Though many of the technologies discussed in Chapter 4 are intended to reduce the likelihood and extent of outages, many of these technologies also directly aid in the restoration stage. Improvements from advanced sensing, controls, and analytics have reduced outages and quickened restoration. In particular, distribution system automation and adaptive islanding are examples of where these technologies can play a role in improving restoration. Further, while these technologies help in the resilience of the electric system, these technologies also improve the reliability of the system to small, localized outages.

### Improving Resilience by Learning from Past Events

The final step in restoration is to reflect on and analyze the experience to improve future restoration efforts. Often restoration from a large-area, long-duration outage is viewed as a unique effort. Nonetheless, it is certain that, even in the midst of a great disaster, another similar outage will follow. In 2005, Katrina seemed a nonpareil event, but Superstorm Sandy followed a mere 7 years later. The industry can and must plan for disaster recovery, but only real disasters stress the plans and expose their gaps and weaknesses. Disasters provide a genuinely unique opportunity to learn.

For most large-area, long-duration outages, there is an after-action report that, for the most part, reads like a historical piece rather than a technical study aimed at process improvement. These reports accurately describe what occurred and what was done (when, where, and by whom) as well as contain a number of short narratives related to particular successes or failures. While this information is useful, even essential, the idiosyncratic approaches make it difficult to identify more general process improvements across multiple events. Outside of the electricity industry, other sectors have developed sophisticated investigation procedures and even maintain full-time, well-trained staff whose only job is to investigate major incidents. The National Transportation Safety Board Investigative Process<sup>8</sup> is solely focused on improving safety and since the Board has no regulatory or enforcement powers, its conclusions cannot be used in litigation. The committee believes that the electricity sector can improve its own investigations by learning from the National

<sup>8</sup> The National Transportation Safety Board Investigative Process is described at <https://www.nts.gov/investigations/process/Pages/default.aspx>, accessed July 11, 2017.



*RESTORING GRID FUNCTION AFTER A MAJOR DISRUPTION*

Transportation Safety Board and potentially creating a similar institutional structure.

Part of the problem is the lack of a general restoration model to provide a common framework for learning. A simple, initial framework was proposed earlier in this chapter, and extension and elaboration of that framework could be very useful in structuring the learning process. Two additional problems are as follows: (1) There is no national process or organization to systemize the integration of studies, and (2) there is insufficient rigor to data collection. The following sections describe a general process for collecting information on the failures and shortcomings in disaster restoration.

### **Step 1: Compile High-Level Facts That Describe the Event**

Step 1 is performed by the study team. A summary should be prepared detailing the essential known facts, including a description of the event, high-level summary of known impacts (e.g., where power was lost and for how long), the grid-level drivers of power loss, the organizations involved with restoration and their activities, a timeline of restoration activities, notable successes and failures, and a list of questions raised. From these facts, a series of maps, organization charts, and information flow diagrams should be prepared. This will provide a guide for the research and a common understanding of the event that can be shared among all of the participants in the research.

### **Step 2: Conduct Interviews**

Beginning with the above summary, a series of interviews with a large number of individuals from all organizations involved in the restoration should be undertaken by the study team. The interviews should focus on what the organization did, as well as its inputs and outputs.

### **Step 3: Perform Synthesis**

The synthesis phase is conducted by the study team and supplemented by subject-matter experts as needed. The synthesis phase extends the event summary by using information from the interviews. The results are summarized in a narrative that incorporates a number of graphics. The graphics include an “entity relationship diagram” (ERD); diagrams of material flows, equipment flows, and information flows; and any other charts the study team deems necessary. The ERD is crucial, as it lists all of the entities involved in restoration, from government, utility, and other private sector groups, and documents their interactions through arrows. For example, the governor’s office (entity) may direct (relationship) to the National Guard (entity). The actual flows of material, equipment, and information overlay the ERD. The reduction of the narrative to these artifacts ensures rigor in and understandability of the analysis.

### **Step 4: Conduct Special Engineering Studies**

Special engineering studies are conducted by technical teams assembled for each study. Electrical disasters and remediation are, to a large extent, studies in organization, communication, and coordination. They are at root, however, serious exercises in engineering. Much of the process described here is directed at organizational and process improvement, which is important because it underpins the response to all disasters, but it is just as important to learn about the design and operation of the grid. These elements must be part of the learning process. Based on the recommendations of the interviews, special engineering studies should be initiated. An example that is particularly important is in understanding the transmission grid. Despite its immense scale, it is a precision machine that requires careful harmonization. The studies may look at things like cyber and physical black start, the repair of analog versus digital components in flooded substations, repair of underground laterals in flooded areas, structure failure mode and possibly the need for redesign, and a host of other subjects. Special subjects should be defined in the study phase when they are essential to understanding the restoration or when the restoration presents an opportunity to learn about the grid and how to improve it. Superstorm Sandy provided an unparalleled opportunity to study grid physics at a large scale, and Katrina provided may examples of restoration of flooded substations.

### **Step 5: Review and Distribute Widely**

All parties involved in grid restoration should be involved in review and socialization. This includes individuals and organizations not impacted by the disaster or involved in its restoration. The synthesis report should be widely distributed and reviewed at meetings in a process of improvement and refinement. This will likely span several months.

### **Step 6: Generalize and Integrate**

This step is conducted by a team developed specifically for this purpose but should involve a few members of the study team. The purpose of the final step is to take the specific analysis that comes from Step 5 and use it to improve the general restoration model, asking which lessons have value beyond simply understanding what occurred.

### **Special Studies—Cascading Failures on the Bulk Power System**

The reliability of U.S. electric power systems has been high enough that the rare occurrences of major blackouts have been prominent national and even international news items. Often, the circumstances leading up to a major system failure include multiple individual factors, each of which alone would have little or no significant impact but when

combined conspire to impact the integrity of the system. In the past, such combinations have resulted through coincident occurrence of unrelated events. For example, during the August 14, 2003, blackout, there were four root causes identified (UCPSOTF, 2004). In the future, events could also be brought together through malevolent synergy. The job of an outage investigation team is to sift through all of the evidence to determine the root causes of the larger system failure and extract lessons for future improvement.

The first step in investigating an incident is to accurately reconstruct the sequence of events. Determining the sequence of events can be a time-consuming process. The first step is gathering all of the data to support the investigation team's evidence-building process (Dagle, 2006). Myriad data sources can provide useful information to support this phase of the investigation. Among the most valuable sources of information are operational logs, records of sequence of events, digital fault recorder output, protective relaying event information, synchrophasor data history, and other similar records of real-time information. The accuracy and precision of these event logs can be critical during cascading events, allowing investigators to sift through the initiating actions and subsequent responses. In the past, significant difficulties have arisen in gathering the data to support the investigation team (Dagle, 2004). The good news is that with the advent of modern power system measurement technology, it is becoming much easier to collect data with microsecond-class measurement accuracy, which is often of ample temporal resolution to be able to accurately determine the sequence of events.

Once the sequence of events is organized, it is valuable to separate it into slower events leading up to the cascading failure and faster events that are occurring during the cascading failure itself. Normally the role of human operators is only relevant during the slower events, and automatic controls are involved in the faster sequences associated with the later stages of the cascading failure.

Particularly with the automated controls, it is necessary to understand the relationship among the various steps in the sequence of events. Characterizing the reason behind any automatic control action helps to develop a deeper understanding of the sequence of events and the chain of events that led up to the cascading failure sequence. This often involves a detailed assessment of protection and other control devices to determine why they operated as well as how their operation contributed to subsequent actions in the sequence of events.

Finally, after considering the sequence of events, and earlier actions that contributed to later actions, the process of root cause determination can be made. It is important in this process to understand that actions taken in advance of the event could be a key root cause finding. For example, inadequate vegetation management, rather than a ground fault to a tree, might be a root cause.

Another important consideration is the degree to which infrastructure damage will prevent rapid restoration of

electricity service. As disruptive as widespread blackouts can be, much worse events are possible. Under several different types of circumstances, electric power systems could be damaged well beyond the level of normal design criteria for maintaining reliability (OTA, 1990). The threats of terrorism, severe storms, and other phenomena, such as geomagnetic disturbances, have increasingly become major concerns to the government and the commercial utility industry. The regulations and policies to mandate how the nation would respond to such an event, or even define who is in charge, are still evolving.

**Finding:** Analysis of large-area, long-duration outages requires an enormous amount of high-precision data. Provision for the collection of these data could be in place before an event. Fundamentally, it is the responsibility of each organization involved in operating the system to conduct event investigations, gather lessons learned, and apply those lessons to minimize the likelihood of subsequent similar events. NERC has jurisdiction and responsibility to conduct investigations of outages involving the bulk power system. Particularly for events that involve multiple organizations, NERC brings tremendous value to the process by assembling outside expertise that cuts across organizational boundaries.

**Recommendation 6.15:** The North American Electric Reliability Corporation, the Federal Energy Regulatory Commission, and relevant regional- and state-level organizations should improve the investigation process of large-scale losses of power with the objective of disseminating lessons across geographical and jurisdictional boundaries. Experiences from outside organizations such as the National Transportation Safety Board should inform this work. To further improve the investigation process, the committee recommends that organizations involved in electricity system operation improve restoration through the following:

- Better and more uniform calibration of recording instruments, including precise time synchronization.
- Pre-defined data requirements to support incident investigations using standard data formats.
- Pre-work logistical details (e.g., prior establishment of confidentiality agreements).
- Infrastructure to support centralized blackout investigations.
- Creation of a data warehouse with servers and databases to store and process the incoming data, support the investigation team, and manage data inventory.
- Defined data categories (to readily track and follow-up on data gaps).
- Automated disturbance reporting.
- Routine collection of transmission and generation events.

## RESTORING GRID FUNCTION AFTER A MAJOR DISRUPTION

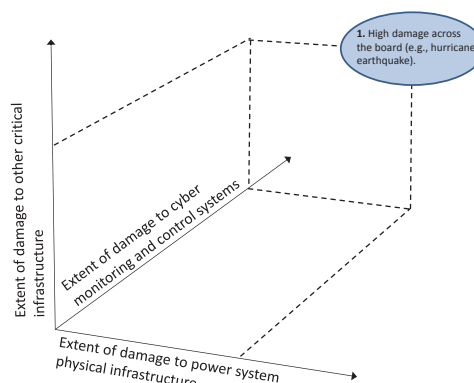
- Improved mechanics of data formats, exchange protocols, and confidentiality issues that can be worked out and tested on an ongoing basis.
- Blackout data that are collected in a matter of hours rather than a matter of days or weeks.

## REFERENCES

- Ball, B. 2006. Rebuilding electrical infrastructure along the Gulf Coast: A case study. *The Bridge: Linking Engineering and Society* 36(1): 21–26.
- CREC (Cuivre River Electric Cooperative). 2016. “Power Restoration Plan.” <https://www.cuivre.com/content/power-restoration-plan>. Accessed July 17, 2017.
- Dagle, J.E. 2004. Data management issues associated with the August 14, 2003 blackout investigation. *IEEE Power Engineering Society General Meeting* 2: 1680–1684.
- Dagle, J.E. 2006. Postmortem analysis of power grid blackouts: The role of measurement systems. *IEEE Power & Energy Magazine* 4(5): 30–35.
- DHS (Department of Homeland Security). 2012. *Recovery Transformer (RecX) Demonstration* [Video file]. <https://www.dhs.gov/science-and-technology/recx-demo-video>. Accessed July 11, 2017.
- DHS. 2014. *Considerations for a Power Transformer Emergency Spare Strategy for the Electric Utility Industry*. <https://www.dhs.gov/sites/default/files/publications/RecX%20-%20Emergency%20Spare%20Transformer%20Strategy-508.pdf>.
- DHS. 2016. *National Response Framework*. 3rd Edition. <https://www.fema.gov/national-response-framework>. Accessed July 13, 2017.
- DOE (Department of Energy). 2015. “Modernizing the Electric Grid.” *Quadrennial Energy Review First Installment: Transforming U.S. Energy Infrastructures in a Time of Rapid Change*. <http://energy.gov/epsa/downloads/quadrennial-energy-review-first-installment>. Accessed July 13, 2017.
- DOE. 2016. *Promoting Innovation for the Design of More Flexible Large Power Transformers*. <https://energy.gov/oe/articles/promoting-innovation-design-more-flexible-large-power-transformers>. Accessed July 11, 2017.
- DOE. 2017. *Quadrennial Energy Review: Transforming the Nation's Electricity System: The Second Installment of the QER*. <https://energy.gov/epsa/downloads/quadrennial-energy-review-second-installment>. Accessed July 13, 2017.
- EEI (Edison Electric Institute). 2016. *Understanding the Electric Power Industry's Response and Restoration Process*. [http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/documents/ma\\_101final.pdf](http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/documents/ma_101final.pdf).
- EPRI (Electric Power Research Institute). 2010. “Development of Power System Restoration Tool Based on Generic Restoration Milestones.” <https://www.epri.com/#/pages/product/000000000001020055/>. Accessed July 13, 2017.
- EPRI. 2012. “Coordinated Cyber-physical Attacks, High-Impact Low-Frequency (HILF) Events, and Risk Management in the Electric Sector.” <http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001025861>. Accessed July 13, 2017.
- EPRI. 2013. “Enhancing Distribution Resiliency: Opportunities for Applying Innovative Technologies.” <https://www.epri.com/#/pages/product/000000000001026889/>. Accessed March 17, 2017.
- ESCC (Electricity Subsector Coordinating Council). 2016. “Overview.” <http://www.electricitysubsector.org/>. Accessed December 15, 2016.
- Fugate, W.C. 2012. “Hurricane Sandy: Response and Recovery Progress and Challenges.” Hearing Before a Subcommittee of the Committee on Appropriations, United States Senate, 112th Congress, December 5.
- Lacey, S. 2014. “Resiliency: How Superstorm Sandy Changed America's Grid.” *GreentechMedia*, June 10. <https://www.greentechmedia.com/articles/featured/resiliency-how-superstorm-sandy-changed-americas-grid>. Accessed July 13, 2017.
- Mandiant. 2016. “M-Trends.” <https://www2.fireeye.com/PPC-m-trends-2016-trends-statistics-mandiant.html>. Accessed July 11, 2017.
- Miller, C., M. Martin, D. Pinney, and G. Walker. 2014. *Achieving a Resilient and Agile Grid*. [http://www.electric.coop/wp-content/uploads/2016/07/Achieving\\_a\\_Resilient\\_and\\_Agile\\_Grid.pdf](http://www.electric.coop/wp-content/uploads/2016/07/Achieving_a_Resilient_and_Agile_Grid.pdf).
- NASEM (National Academies of Sciences, Engineering, and Medicine). 2016. *Electricity Use in Rural and Islanded Communities: Proceedings of a Workshop*. Washington, D.C.: The National Academies Press.
- NERC (North American Electric Reliability Corporation). 2016a. *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans*. <https://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf>.
- NERC. 2016b. *Grid Security Exercise*. <http://www.nerc.com/pa/CI/CIP Outreach/GridEX/NERC%20GridEx%20III%20Report.pdf>.
- NRC (National Research Council). 2012. *Terrorism and the Electric Power Delivery System*. Washington, D.C.: The National Academies Press.
- NYSEG (New York State Electric and Gas Corporation) and RGEC (Rochester Gas and Electric Corporation). 2016. *Electricity Utility Emergency Plan*. <https://www.nyseg.com/MediaLibrary/2/5/Content%20Management/Shared/SuppliersPartners/PDFs%20and%20Docs/NYSEG%20and%20ERGE%20Electric%20Utility%20Emergency%20Plan.pdf>.
- Olearczyk, M. 2013. *Airborne Damage Assessment Module (ADAM)*. Electric Power Research Institute 2013 Distribution System Research Portfolio. [http://mydocs.epri.com/docs/Portfolio/PDF/2013\\_P180.pdf](http://mydocs.epri.com/docs/Portfolio/PDF/2013_P180.pdf).
- OTA (Office of Technology Assessment). 1990. *Physical Vulnerability of Electric System to Natural Disasters and Sabotage, OTA-E-453*. Washington, D.C.: U.S. Government Printing Office.
- Parfomak, P.W. 2014. *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*. <https://fas.org/sgp/crs/homesecc/R43604.pdf>.
- PJM. 2016. “PJM Manual 36: System Restoration.” <http://www.pjm.com/~media/documents/manuals/m36.ashx>. Accessed July 13, 2017.
- UCPSOTF (U.S.–Canada Power System Outage Task Force). 2004. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendation*. <https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>.

## ANNEX TABLES

**TABLE 6A.1** Variation in Restoration Activities Across the Six Stages of the Life Cycle of an Outage Characterized by Damage to Physical Components, Monitoring and Control Systems, and Supporting Infrastructure, As Indicated in the Upper Right Corner of Figure 3.2



	Hurricanes and Tropical Storms	Floods
	<p>Area impacted: Typically very large</p> <p>Damage to aboveground assets: Poles, towers, substations</p> <p>Damage to customer assets: Extensive</p> <p>Limits to access and mobility: Major blockage</p> <p>Event warning: Days</p> <p>Risk assessment: Can be identified beforehand</p> <p>Rate of propagation: Slow</p>	<p>Area impacted: Typically very large</p> <p>Damage to aboveground assets: Poles, towers, substations</p> <p>Damage to customer assets: Extensive</p> <p>Limits to access and mobility: Major blockage</p> <p>Event warning: Days</p> <p>Risk assessment: Can be identified beforehand</p> <p>Rate of propagation: Slow</p>
<b>Plan</b>	<p>Individual utilities plan for hurricanes and tropical storms based on their experience and historical hurricane tracks, although these tracks may be trending more northerly in the Atlantic, placing the Mid-Atlantic states and New England at greater risk than in the past. Utilities are experts in identifying their specific vulnerable assets. During this phase, utilities should establish and refresh mutual aid agreements, create owned and shared inventory, train crews, conduct exercises, and communicate with customers regarding emergency preparedness.</p>	<p>More than any other disaster, floods are subject to statistical analysis, and utilities plan based on FEMA flood maps. Some adjustment should be made if there has been substantial reduction in forest cover or if there has been substantial development in the impacted watershed. Consideration should also be given to how, in light of climate change, future flood risk may be different from historical risk. To the extent possible, critical assets should not be located in identified flood plains, but there are numerous legacy assets exposed to flood risk. Floods in major river basins tend to be slow rising and slow receding, with lesser hydrostatic force. In contrast, canyon flooding (largely in western mountains) tends to be fast rising with short notice, forceful, and quick to recede. In either case, assets at risk can be identified and measures taken to reduce risk such as elevating them above the flood or building coffer dams. Plans should be made to replace assets in flood plains.</p>
<b>Prepare</b>	<p>Hurricane wind and rain forecasts with high uncertainty are available up to 1 week in advance, which is sufficient time to elevate or downgrade risk. When risk is elevated, staffing for the emergency can be refined, and mutual aid agreements can be activated. Flood forecasts are available only 3 to 4 days in advance, and peak flooding frequently follows the event.</p>	<p>River basin flood forecasts are available 3 to 4 days in advance. Many flash floods occur with effectively no warning; however, if major rain events are forecast for canyon areas, utilities may place crews on standby. When a flood is forecast in a river basin, it is possible to forecast which areas and assets are most likely to be affected. General restoration plans can be made more specific, and mutual aid agreements and emergency operations centers can be activated. Lists of materials, supplies, and equipment can be developed, procured, and staged.</p>
<b>Event</b>	<p>Relatively little can be done on distribution systems during the comparatively short duration of the event. Transmission systems must be adjusted as loads, generators, and transmission lines drop off the grid. Utilities develop an understanding of the extent of damage and customer outages and develop specific plans for remediation, building on the general planning. Government support organizations monitor conditions and establish and exercise lines of communications with utilities and with each other. Limited actions should be taken by utilities only when safety is an issue.</p>	<p>Major river floods are long-duration events that move down a river basin. Restoration can start upstream while the event is still evolving downstream, and some protective measures can be undertaken as water rises. Before restoration begins in an area, the plans can be improved and refined with emphasis on the temporal sequencing. Communications and coordination should be established and exercised.</p>



	Hurricanes and Tropical Storms	Floods
<b>Endure</b>	The endurance phase is the period from when the storm passes to the start of restoration. Unless there is flooding, restoration can begin immediately. If there is a delay, the time should be spent moving crews into position to the extent that the condition of the roads and safety considerations allow. Effort should also be made to improve the assessment of the state of conditions, to refine plans, and to refine requests for support from and coordination with other organizations, including other utilities and government organizations. This involves the high level such as governors' offices, but also the crews on the ground, as per informing police and fire departments about the utility staff who will be working in their area. If specialized equipment is needed, arrangements should be made for acquisition and staging for deployment.	The endurance phase for a flood at one point can be very short in areas where the grade of a river is steeper or long in low-lying flat areas. Work begins in an area as soon as the water recedes, allowing restoration.
<b>Restore</b>	Restoration is the most visible phase of the event. Crews are on the streets working. While this is a difficult and costly phase, it is one that most utilities are familiar with and good at. If there are many trees and other obstacles in the street, they must be cleared to gain access to facilities. Utilities and the linemen know how to clear access, set poles, erect towers, string conductors, and clean and repair substations. The goal of management and support organizations (including governmental) is to ensure that the line crews are used effectively. They must be dispatched to the areas where their work will have the greatest impact, considering what is doable, and placed in a sequence of restoration activities. Management should work the supply chain to be sure that crews have the equipment, parts, and supplies (including fuel) they need to execute the necessary repairs. Crews must be provided with provisions, including food and housing, and amenities, such as electrical and phone service and access to health services for the injuries that are inevitable in this dangerous physical work. Experience has shown that taking care of the families left behind when crews are deployed is an important factor in enabling them to work effectively.	Flood restoration can take a very long time. In the absence of wind, poles and towers are not typically damaged; nonetheless, the ground can be softened and some distribution and transmission failures may occur. Manholes are flooded and must be pumped out. Underground lines and associated gear sometimes survive intact but often are damaged to the point of needing costly and time-consuming replacement. Flooded substations are difficult to restore. Analog equipment can sometimes be cleaned, dried, and returned to service, but digital devices typically need replacement. Underground vaults are problematic as they are difficult to drain and dry, can accumulate deep mud, and are more difficult to move equipment in and out of. All of this, however, is work utilities know and are well equipped to manage. The key, as noted in the discussion of hurricanes, is to provide broad support to the crews.
<b>Recover</b>	Hurricanes damage communities, not just utilities. Utilities must be part of the community restoration, perhaps lasting years. Rebuilding is an opportunity for improving.	Floods damage communities, not just utilities. Utilities must cooperate with other entities in the restoration as, for example, in repairing or replacing civil and safety infrastructure.
	Earthquakes	Winter Storms
	Area impacted: Limited to extensive Damage to aboveground assets: Poles, towers, substations Damage to customer assets: Limited to extensive Limits to access and mobility: Major blockage Event warning: Seconds to minutes Risk assessment: Difficult Rate of propagation: Fast	Area impacted: Regional Damage to aboveground assets: Lines, poles, towers Damage to customer assets: Limited Limits to access and mobility: Potential blockage Event warning: Days Risk assessment: Straightforward Rate of propagation: Slow
<b>Plan</b>	Earthquake risk is well mapped, and utilities routinely consider earthquake risk in siting and planning processes. Methods for earthquake-survivable construction are well researched. Major plants (e.g., North Anna Nuclear Power Station) have survived earthquakes with no damage, though safety considerations have taken them off-line for an extended period. Planning consists of maintaining adequate parts inventories.	Utilities operating in regions subject to winter storms often design systems components, such as transmission towers and lines, to be able to withstand greater amounts of precipitation and wind compared to other areas.
<b>Prepare</b>	There is work on developing a near-term warning capability for earthquakes, but presently most occur with no useful warning.	Winter storm forecasts provide several days' warning that allows for arrangement of mutual aid.
<b>Event</b>	Earthquakes are of short duration. No action during the earthquake is practical.	Some final preparation is possible during the event as outages are mapped. Transmission system operators must rebalance to accommodate failing loads and distribution systems.
<b>Endure</b>	Restoration can begin immediately.	Delay in the start of restoration is possible if the roads are blocked or ice-covered.

*continued*

TABLE 6A.1 Continued

	Earthquakes	Winter Storms
<b>Restore</b>	Restoration consists of familiar utility construction but can be severely hampered by damage to supporting infrastructure. Roads and bridges can be blocked or torn away, natural gas pipelines can break, and fuel storage can rupture. Electricity system restoration is executed as part of a broader restoration effort, and coordination among federal, state, and local government, as well as utility decision makers, is essential. Shortages of materials and equipment may result in competition for scarce resources, and availability will vary geographically. Even access to food and water may be a challenge in some remote areas. There is substantial risk that the homes and families of crews may be impacted or imperiled, undermining their ability to commit to utility restoration activities. Mutual aid from unaffected areas is essential.	Restoration following winter storms is standard utility work. Mutual aid is beneficial, and due to the generally smaller geographic extent of such storms, there are fewer issues in supporting the crews or marshalling supplies than are faced during restoration from hurricanes and earthquakes. Cold temperatures do reduce effectiveness of line crews.
<b>Recover</b>	Utility restoration can be completed well in advance of the general commercial and civil infrastructure. Utility capabilities are enablers of recovery.	Winter storms do not typically inflict lasting damage on infrastructure and enablers of economic recovery.
	Tornadoes	Geomagnetic Disturbances
	Area impacted: Limited to clustered Damage to aboveground assets: Poles, towers, substations Damage to customer assets: Serious but contained Limits to access and mobility: Minor blockage Event warning: Seconds to minutes Risk assessment: Regionally known Rate of propagation: Fast	Area impacted: Very large Damage to aboveground assets: Transformers, substations Damage to customer assets: Limited Limits to access and mobility: None Event warning: Minutes to days Risk assessment: Costly Rate of propagation: Very fast
<b>Plan</b>	Utilities in high-risk areas are aware of the peril and have likely dealt with tornadoes in the past. The focus in planning is on inventory of aboveground assets and mutual assistance. Unlike some other causes, transmission and generation assets are at risk of damage from tornadoes.	Risk assessment is nascent and based on highly uncertain estimates of frequency and intensity, but methods to harden the grid are available. Replacement transformers and other vulnerable components can be stockpiled but may be too expensive to be forward deployed.
<b>Prepare</b>	The incidence of weather conditions likely to spawn tornadoes can be provided 1 day to several hours in advance. There is little time to prepare, except to bring crews to a state of readiness and fully man response centers.	Solar weather warning systems can provide some notice, allowing for minimal preparation, but there is generally insufficient time to move crews.
<b>Event</b>	Events are of such short duration that there is no practical action during the event, except that transmission operators may have to adjust to limit impact.	The building up of current on long lines can trigger operational changes to protection systems, particularly shedding load to desaturate transformers.
<b>Endure</b>	Restoration can generally begin immediately after the event passes.	Restoration can begin immediately.
<b>Restore</b>	Customer property may be destroyed alongside utility assets, which means that there may be no immediate need to restore power to the affected area. Nonetheless, the tornado may damage a transmission corridor or section of the distribution grid essential to providing service to unaffected areas. The work is familiar to utilities and, in the case of tornadoes, the impact is sufficiently localized that there is less difficulty in provisioning and supporting crews. There are likely to be intact facilities within a few miles or tens of miles of the worksite.	There is no precedent for a large-scale geomagnetic disturbance event. If the impact is very large, there may be shortages of major components, particularly large transformers due to the long lead time in building and acquiring these.
<b>Recover</b>	Tornadoes do very serious damage to the impacted community so that the recovery period can be extensive after the immediate restoration is completed. Utilities must participate in planning this recovery.	Recovery is not a factor. Extensive damage beyond the grid is unlikely since long lines are needed to build damaging current level.

**TABLE 6A.2** Restoration Activities Across the Six Stages of the Life Cycle of an Outage from a Cyber Attack

Area Impacted	Feeder Level to System Level
Damage to aboveground assets	Cyber assets will certainly be compromised, perhaps beyond restoration. Control actions initiated by the pernicious actor may create a wide range of physical damage up to and including generators. In addition, “smart” components may be compromised in a way that they are no longer controllable. Such damage may be irreversible or compromise trust in the device so that it may not be used safely. This damage to the electronic aspects of a device is functionally equivalent to physical damage.
Damage to customer assets	Limited except, possibly, to smart meters. Meters are owned by the utility but are associated with a specific customer. If the meter includes a local wireless connection for home automation, there are potential attack strategies which may do damage to customer systems, but no such Internet of Things attack has been successful.
Limits to access and mobility	None.
Event warning	Potentially months.
Risk assessment	Cyber N-1 and N-2 analyses should become standard practice.
Rate of propagation	Slow from breach to first action, very fast from first action.
<b>Plan</b>	Planning for cyber attack is a routine part of utility operations. It tends to focus, however, on prevention rather than restoration. The emphasis in restoration is on reestablishing the operational capability of sensor, computational, and communications assets; reestablishing state; and gaining confidence in the integrity of the systems and the information they manage. Planning for cyber restoration should be planned and practiced.
<b>Prepare</b>	Systems must be improved to react more effectively to new threat information. Updated threat information is provided daily, but the systems to move this information into quick action at a utility cannot make immediate use of the information. Much of it must work its way through cybersecurity software and service providers.
<b>Event</b>	A cyber event may last several months. During the period from breach to action, the utility may be able to sever access by malicious actors, preventing damage.
<b>Endure</b>	Restoration can begin immediately on detection.
<b>Restore</b>	Methods for manual operation and restoration systems should be developed in advance. Fast reaction cyber teams should be on call.
<b>Recover</b>	Not applicable.

## 7

## Conclusions

No single entity is responsible for, or has the authority to implement, a comprehensive approach to assure the resilience of the nation's electricity system. Chapter 2 described the complex structure, asset ownership, and regulatory system of the current electricity system and how the changing nature of the electricity system provides both opportunities and challenges for system resilience. Because most parties are preoccupied dealing with short-term issues, they neither have the time to think systematically about what could happen in the event of a large-area, long-duration blackout, nor do they adequately consider the consequences of large-area, long-duration blackouts in their operational and other planning or in setting research and development priorities. Hence the United States needs a process to help all parties better envision the consequences of low-probability but high-impact events precipitated by the causes outlined in Chapter 3 and the system-wide effects discussed in Chapter 5. The specific recommendations addressed to particular parties that are provided in the report (especially in Chapters 4 through 6) will incrementally advance the cause of resilience. However, these alone will be insufficient unless the nation is able to adopt a more integrated perspective at the same time. Thus, this chapter provides a series of overarching recommendations that build upon the detailed recommendations contained within this report.

### OVERARCHING INSIGHTS AND RECOMMENDATIONS

The first strategy that should be pursued to enhance the resilience of the system is to make sure that things already in place will work when they are needed. One of the best ways to do that is to conduct drills with other critical infrastructure operators through large-scale, multisector exercises. Such exercises can help illuminate areas where improvements in processes and technologies can substantively enhance the resilience of the nation's critical infrastructure.

**Overarching Recommendation 1:** Operators of the electricity system, including regional transmission organizations,

investor-owned utilities, cooperatives, and municipally owned utilities, should work individually and collectively, in cooperation with the Electricity Subsector Coordinating Council, regional and state authorities, the Federal Energy Regulatory Commission, and the North American Electric Reliability Corporation, to conduct more regional emergency preparedness exercises that simulate accidental failures, physical and cyber attacks, and other impairments that result in large-scale loss of power and/or other critical infrastructure sectors—especially communication, water, and natural gas. Counterparts from other critical infrastructure sections should be involved, as well as state, local, and regional emergency management offices.

The challenges that remain to achieving grid resilience are so great that they cannot be achieved by research- or operations-related activities alone. While new technologies and strategies can improve the resilience of the power system, many existing technologies that show promise have yet to be fully adopted or implemented. In addition, more coordination between research and implementation activities is needed, building on the specific recommendations made throughout this report. Immediate action is needed both to implement available technological and operational changes and to continue to support the development of new technologies and strategies.

**Overarching Recommendation 2:** Operators of the electricity system, including regional transmission organizations, investor-owned utilities, cooperatives, and municipals, should work individually and collectively to more rapidly implement resilience-enhancing technical capabilities and operational strategies that are available today and to speed the adoption of new capabilities and strategies as they become available.

The Department of Energy (DOE) is the federal entity with a mission to focus on the *longer-term* issues of developing and promulgating technologies and strategies to increase



## CONCLUSIONS

the resilience and modernization of the electric grid.<sup>1</sup> At present, two offices within DOE have responsibility for issues directly and indirectly related to grid modernization and resilience.

**Overarching Recommendation 3:** However the Department of Energy chooses to organize its programs going forward, Congress and the Department of Energy leadership should sustain and expand the substantive areas of research, development, and demonstration that are now being undertaken by the Department of Energy's Office of Electricity Delivery and Energy Reliability and Office of Energy Efficiency and Renewable Energy, with respect to grid modernization and systems integration, with the explicit intention of improving the resilience of the U.S. power grid. Field demonstrations of physical and cyber improvements that could subsequently lead to widespread deployment are critically important. The Department of Energy should collaborate with parties in the private sector and in states and localities to jointly plan for and support such demonstrations. Department of Energy efforts should include engagement with key stakeholders in emergency response to build and disseminate best practices across the industry.

The U.S. grid remains vulnerable to natural disasters, physical and cyber attacks, and other accidental failures.

**Overarching Recommendation 4:** Through public and private means, the United States should substantially increase the resources committed to the physical components needed to ensure that critical electric infrastructure is robust and that society is able to cope when the grid fails. Some of this investment should focus on making the existing infrastructure more resilient and easier to repair, including the following:

- The Department of Energy should launch a program to manufacture and deploy flexible and transportable three-phase recovery transformer sets that can be pre-positioned around the country.<sup>2</sup> These recovery transformers should be easy to install and use temporarily

<sup>1</sup> The Department of Homeland Security, the Federal Energy Regulatory Commission, and other organizations also provide critical support and have primacy in certain areas.

<sup>2</sup> As noted in Chapter 6 and in the next section of this chapter, the DOE Office of Electricity Delivery and Energy Reliability is supporting the development of a new generation of high-voltage transformers that will use power electronics to adjust their electrical properties and hence can be deployed in a wider range of settings. The committee's recommendation to manufacture recovery transformers is not intended to replace that longer-term effort. However, the new DOE advanced transformer designs will not be available for some time, and in the meantime the system remains physically vulnerable. While in Chapter 6 the committee notes several government and industry-led transformer-sharing and recovery programs, the committee recognizes that high-voltage transformers represent one of the grid's most vulnerable components deserving of further efforts.

until conventional transformer replacements are available. This effort should produce sufficient numbers (on the order of tens compared to the three produced by the Department of Homeland Security's RecX program) to provide some practical protection in the case of an event that results in the loss of a number of high-voltage transformers. This effort should complement instead of replace ongoing initiatives related to spare transformers.

- State and federal regulatory commissions and regional transmission organizations should then evaluate whether grids under their supervision need additional pre-positioned replacements for critical assets that can help accelerate orderly restoration of grid service after failure.
- Public and private parties should expand efforts to improve their ability to maintain and restore critical services—such as power for hospitals, first responders, water supply and sewage systems, and communication systems.<sup>3</sup>
- The Department of Energy, the Department of Homeland Security, the Electricity Subsector Coordinating Council, and other federal organizations, such as the U.S. Army Corps of Engineers, should oversee the development of more reliable inventories of backup power needs and capabilities (e.g., the U.S. Army Corps of Engineers' mobile generator fleet), including fuel supplies. They should also "stress test" existing supply contracts for equipment and fuel supply that are widely used in place of actual physical assets in order to be certain these arrangements will function in times of major extended outages. Although the federal government cannot provide backup power equipment to everyone affected by a large-scale outage, these resources could make significant contributions at select critical loads.

In addition to providing redundancy of critical assets, transmission and distribution system resilience demands the ability to provide rapid response to events that impair the ability of the power system to perform its function. These events include deliberate attacks on and accidental failures of the infrastructure itself, as well as other causes of grid failure, which are discussed in Chapter 3.

**Overarching Recommendation 5:** The Department of Energy, together with the Department of Homeland Security, academic research teams, the national laboratories, and companies in the private sector, should carry out a program of research, development, and demonstration activities to

<sup>3</sup> In addition to treatment, sewage systems often need to pump uphill. A loss of power can quickly lead to sewage backups. Notably, a high percentage of the hospital backup generators in New York City failed during Superstorm Sandy.

improve the security and resilience of cyber monitoring and controls systems, including the following:

- Continuous collection of diverse (cyber and physical) sensor data;
- Fusion of sensor data with other intelligence information to diagnose the cause of the impairment (cyber or physical);
- Visualization techniques needed to allow operators and engineers to maintain situational awareness;
- Analytics (including machine learning, data mining, game theory, and other artificial intelligence-based techniques) to generate real-time recommendations for actions that should be taken in response to the diagnosed attacks, failures, or other impairments;
- Restoration of control system and power delivery functionality and cyber and physical operational data in response to the impairment; and
- Creation of post-event tools for detection, analysis, and restoration to complement event prevention tools.

Because no single entity is in charge of planning the evolution of the grid, there is a risk that society may not adequately anticipate and address many elements of grid reliability and resilience and that the risks of this system-wide failure in preparedness will grow as the structure of the power industry becomes more atomized and complex. There are many opportunities for federal leadership in anticipating potential system vulnerabilities at a national level, but national solutions are then refined in light of local and regional circumstances. Doing this requires a multi-step process, the first of which is to anticipate the myriad ways in which the system might be disrupted and the many social, economic, and other consequences of such disruptions. The second is to envision the range of technological and organizational innovations that are affecting the industry (e.g., distributed generation and storage) and how such developments may affect the system's reliability and resilience. The third is to figure out what upgrades should be made and how to cover their costs. For simplicity, the committee will refer to this as a "visioning process." While the Department of Homeland Security (DHS) has overarching responsibility for infrastructure protection, DOE, as the sector-specific agency for energy infrastructure, has a legal mandate and the deep technical expertise to work on such issues.

**Overarching Recommendation 6:** The Department of Energy and the Department of Homeland Security should jointly establish and support a "visioning" process with the objective of systematically imagining and assessing plausible large-area, long-duration grid disruptions that could have major economic, social, and other adverse consequences, focusing on those that could have impacts related to U.S. dependence on vital public infrastructures and services provided by the grid.

Because it is inherently difficult to imagine systematically things that have not happened (Fischhoff et al., 1978; Kahneman, 2011), exercises in envisioning benefit from having multiple groups perform such work independently. For example, such a visioning process might be accomplished through the creation of two small national power system resilience assessment groups (possibly at DOE national laboratories and/or other federally funded research and development centers or research universities). However such visioning is accomplished, engagement from staff representing relevant state and federal agencies is essential in helping to frame and inform the work. These efforts should build on the detailed recommendations in this report to identify technical and organizational strategies that increase electricity system resilience in numerous threat scenarios—that is, by preventing and mitigating the extent of large-scale grid failures, sustaining critical services in the instance of failure, and recovering rapidly from major outages—and to assess the costs and financing mechanisms to implement the proposed strategies. Attention is needed not just to the average economy-wide costs and benefits, but also to the distribution of these across different levels of income and vulnerability. It is important that these teams work to identify common elements in terms of hazards and solutions so as to move past a hazard-by-hazard approach to a more systems-oriented strategy. Producing useful insights from this process will require mechanisms to help these groups identify areas of overlap while also characterizing the areas of disagreement. A consensus view could be much less helpful than a mapping of uncertainties that can help other actors—for example, state regulatory commissions and first responders—understand the areas of deeper unknowns.

National labs, other federally funded research and development centers, and research universities do not operate or regulate the power system. At the national level, the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) both have relevant responsibilities and authorities.

**Overarching Recommendation 7A:** The Federal Energy Regulatory Commission and the North American Electric Reliability Corporation should establish small system resilience groups, informed by the work of the Department of Energy/Department of Homeland Security "visioning" process, to assess and, as needed, to mandate strategies designed to increase the resilience of the U.S. bulk electricity system. By focusing on the crosscutting impacts of hazards on interdependent critical infrastructures, one objective of these groups would be to complement and enhance existing efforts across relevant organizations.

As the discussions throughout this report make clear, many different organizations are involved in planning, operating, and regulating the grid at the local and regional levels. By design and of necessity in our constitutional democracy,

## CONCLUSIONS

making decisions about resilience is an inherently political process. Ultimately the choice of how much resilience our society should and will buy must be a collective social judgment. It is unrealistic to expect firms to make investments voluntarily whose benefits may not accrue to shareholders within the relevant commercial lifetime for evaluating projects. Moreover, much of the benefit from avoiding such events, should they occur, will not accrue to the individual firms that invest in these capabilities. Rather, the benefits are diffused more broadly across multiple industries and society as a whole, and many of the decisions must occur on a state-by-state basis.

**Overarching Recommendation 7B:** The National Association of Regulatory Utility Commissioners should work with the National Association of State Energy Officials to create a committee to provide guidance to state regulators on how best to respond to identified local and regional power system-related vulnerabilities. The work of this committee should be informed by the national “visioning” process, as well as by the work of other research organizations. The mission of this committee should be to develop guidance for, and provide technical and institutional support to, state commissions to help them to more systematically address broad issues of power system resilience, including decisions as to what upgrades are desirable and how to pay for them. Guidance developed through this process should be shared with appropriate representatives from the American Public Power Association and the National Rural Electric Cooperative Association.

**Overarching Recommendation 7C:** Each state public utility commission and state energy office, working with the National Association of Regulatory Utility Commissioners, the National Association of State Energy Officials, and state and regional grid operators and emergency preparedness organizations, should establish a standing capability to identify vulnerabilities, identify strategies to reduce local vulnerabilities, develop strategies to cover costs of needed upgrades, and help the public to become better prepared for extended outages. In addition, they should encourage local and regional governments to conduct assessments of their potential vulnerabilities in the event of large-area, long-duration blackouts and to develop strategies to improve their preparedness.

Throughout this report, the committee has laid out a wide range of actions that different parties might undertake to improve the resilience of the United States power system. If the approaches the committee has outlined can be implemented, they will represent a most valuable contribution. At the same time, the committee is aware that the benefits of such a contribution—avoiding large-scale harms that are rarely observed—are easily eclipsed by the

more tangible daily challenges, pressures on budgets, public attention, and other scarce resources. Too often in the past, the United States has made progress on issues of resilience by “muddling through” (Lindblom, 1959). Even if the broad systematic approach outlined in this report cannot be fully implemented immediately, it is important that relevant organizations develop analogous strategies so that when a policy window opens in the aftermath of a major disruption, well-conceived solutions are readily available for implementation (Kingdon, 1984).

## SUMMARY OF DETAILED RECOMMENDATIONS

Underlying the Overarching Recommendations are the numerous, more targeted recommendations presented throughout this report. Here, the committee summarizes and sorts these recommendations by the institutions to which they are directed.

## Recommendations Directed to the Department of Energy

DOE plays a critical role in enhancing the resilience of the grid through research, development, and demonstration programs as well as convening and engagement activities. Much progress has been made, and DOE should sustain and expand many of these efforts.

**Recommendation 1 to DOE:** Improve understanding of customer and societal value associated with increased resilience and review and operationalize metrics for resilience by doing the following:

- Developing comprehensive studies to assess the value to customers of improved reliability and resilience (e.g., periodic rotating service) during large-area, long-duration blackouts as a function of key circumstances (e.g., duration, climatic conditions, societal function) and for different customer classes (e.g., residential, commercial, industrial). (Recommendation 2.1)
- Conducting a coordinated assessment of the numerous resilience metrics being proposed for transmission and distribution systems and seeking to operationalize these metrics within the utility setting. In doing the review, engagement with key stakeholders is essential. (Recommendation 2.2)

**Recommendation 2 to DOE:** Support research, development, and demonstration activities, as well as convening activities, to improve the resilience of power system operations and recovery by reducing barriers to adoption of innovative technologies and operational strategies. These include the following:

- Coordinating with federal and state utility regulators to support a modest grant program that encourages utility

investment in innovative solutions that demonstrate resilience enhancement. These projects should be selected to reduce barrier(s) to entry by improving regulator and utility confidence. (Recommendation 4.1)

- Initiating and supporting ongoing research programs focused on the operation of degraded or damaged electricity systems, including supporting infrastructure and cyber monitoring and control systems, where key subsystems are designed and operated to sustain critical functionality. (Recommendation 4.6)
- Convening transmission and distribution system owners and operators to engage the Federal Aviation Administration proactively to ensure that the rules regulating operation of unmanned aerial vehicles support the rapid, safe, and effective applications of unmanned aerial vehicle technology in electricity restoration activities, including pre-disaster tests and drills. (Recommendation 6.5)
- Continuing to support research and development of advanced large power transformers, concentrating on moving beyond design studies to conduct several demonstration projects. (Recommendation 6.7)

**Recommendation 3 to DOE:** Advance the safe and effective development of distributed energy resources (DERs) and microgrids by doing the following:

- Initiating research, development, and demonstration activities to explore the extent to which DERs could be used to help prevent large-area outages. (Recommendation 4.2)
- Supporting demonstration and a training facility (or facilities) for future microgrids that will allow utility engineers and non-utility microgrid operators to gain hands-on experience with islanding, operating, and restoring feeders (including microgrids). (Recommendation 5.6)
- Engaging the manufacturers of plug-in hybrid electric and fuel cell vehicles to study how such vehicles might be used as distributed sources of emergency power. (Recommendation 5.12)
- Evaluating the technical and contractual requirements for using DERs as part of restoration activities, even when these assets are not owned by the utility, to improve restoration and overall resilience. (Recommendation 6.3)

**Recommendation 4 to DOE:** Work to improve the ability to use computers, software, and simulation to research, plan, and operate the power system to increase resilience by doing the following:

- Collaborating with other research organizations, including the National Science Foundation, to expand support for interdisciplinary research to simulate

events and model grid impacts and mitigation strategies. (Recommendation 4.3)

- Supporting and expanding research and development activities to create synthetic power grid physical and cyber infrastructure models. (Recommendation 4.4)
- Collaborating with other research organizations, including the National Science Foundation, to fund research on enhanced power system wide-area monitoring and control and the application of artificial intelligence to the power system. Such work should include how the human-computer interface and visualization could improve reliability and resilience. (Recommendation 4.8)
- Leading efforts to develop standardized data definitions, communication protocols, and industrial control system designs for the sharing of both physical and cyber system health information. (Recommendation 4.9)
- Developing a high-performance utility network simulator for use in cyber configuration and testing. (Recommendation 6.12)

**Recommendation 5 to DOE:** Work to improve the cybersecurity and cyber resilience of the grid by doing the following:

- Embarking on a research, development, and demonstration program that results in a prototypical cyber-physical-social control system architecture for resilient electric power systems. (Recommendation 4.10)
- Developing the ability to apply physics-based modeling to anomaly detection, which provides real-time or better physics models that derive optimal power flow and monitor performance for more accurate state estimation. (Recommendation 6.8)

### **Recommendations Directed to the Electric Power Sector and the Department of Energy**

There are thousands of operating utilities and electricity system asset owners across the United States, with diverse characteristics and institutional structures, including private investor-owned utilities, cooperatives, and publicly owned entities. These organizations, and the people they employ, are the foundation of a reliable and resilient grid, and many promising demonstrations and initiatives are ongoing across the sector. The industry and DOE have benefitted from a strong relationship, and the committee encourages further collaboration on projects to increase the resilience of the grid.

**Recommendation 6 to the electric power sector and DOE:** The owners and operators of electricity infrastructure should work closely with DOE as follows:

- Develop use cases and perform research on strategies for intelligent load shedding based on advanced



## CONCLUSIONS

metering infrastructure and customer technologies like smart circuit breakers. (Recommendation 4.5)

- Explore the feasibility of establishing contractual and billing agreements with private owners of DERs and developing the ability to operate intact islanded feeders as islanded microgrids powered by utility- and customer-owned generating resources to supply limited power to critical loads during large grid outages of long duration. (Recommendation 5.10)
- Work together to analyze past large-area, long-duration outages to identify common elements and processes for system restoration and define best practices that can be shared broadly throughout the electricity industry. (Recommendation 6.2)
- Identify those components and corresponding events for which pre-event de-energizing of selected assets is the lowest risk strategy and develop regulatory, communication (especially with customers), and other plans that allow such protective action to be implemented. (Recommendation 6.4)
- Expand joint cyber-physical recovery exercises that emphasize, among other things, the maintenance of cyber protection during the chaotic period of physical restoration. (Recommendation 6.14)

Clearly, some of these recommendations will require greater degrees of DOE engagement than others.

### Recommendations Directed to the Department of Homeland Security and the Department of Energy

Because emergency response and management is central to power system resilience, the committee makes several recommendations that call for collaboration between DHS and DOE.

**Recommendation 7 to DHS and DOE:** DHS and DOE should work collaboratively to improve preparation for, emergency response to, and recovery from large-area, long-duration blackouts by doing the following:

- Working with state and local authorities and electricity system operators to undertake an “all hazards” assessment of the natural hazards faced by power systems on a periodic basis (e.g., every 5 years). Local utilities should customize those assessments to their local conditions. (Recommendation 3.2)
- Developing and overseeing a process to help regional and local planners envision potential system-wide effects of long-duration loss of grid power. (Recommendation 5.3)
- Evaluating and recommending the best approach for getting critical facility managers to pre-register information about emergency power needs and available resources. (Recommendation 5.5)

- Renewing efforts to work with utilities and national, state, and local law enforcement to develop formal arrangements (such as designating selected utility personnel as “first responders”) that credential selected utility personnel to allow prompt utility access to damaged facilities across jurisdictional boundaries. (Recommendation 6.1)
- Building off of existing efforts to manufacture and stockpile flexible, high-voltage replacement transformers, in collaboration with electricity system operators and asset owners and with support from the U.S. Congress. (Recommendation 6.6)
- Developing a model for large-scale cyber restoration of electricity infrastructure. (Recommendation 6.9)

**Recommendation 8 to DHS and DOE:** With growing awareness of the electricity system as a potential target for malicious attacks using both physical and cyber means, DHS and DOE should work closely with operating utilities and other relevant stakeholders to improve physical and cyber security and resilience by doing the following:

- Working with operating utilities to sustain and enhance their monitoring and information-sharing activities to protect the grid from physical and cyber attacks. (Recommendation 3.1)
- Continuing to work with the Electricity Subsector Coordinating Council and operating utilities to enhance the sharing of cyber restoration resources (i.e., cyber mutual assistance agreements), including personnel, focusing on peer-to-peer collaboration as well as engagement with government, industry organizations, and commercial cybersecurity companies. (Recommendation 6.10)
- Working with the electricity sector and representatives of other key affected industries and sectors to continue to strengthen the bidirectional communication between federal cybersecurity programs and commercial software companies. (Recommendation 6.11)
- Redoubling efforts to reduce the vulnerability of the power system to terrorist attacks in close collaboration with FERC, NERC, and other representatives of the electric industry. (Recommendation 6.13)

### Recommendations Directed to State Offices and Regulatory Bodies

State offices and elected officials have an important role in increasing the resilience of the nation's electricity system, including through planning and regulatory decisions as well as emergency preparedness and response. Several of the committee's recommendations encourage various actors in state government to take action.

**Recommendation 9 to state offices and regulators:** Work with local utilities and relevant stakeholders to increase investment in resilience-enhancing strategies, including the following:

- State emergency planning authorities should oversee a more regular and systematic testing of backup power generation equipment at critical facilities, such as hospitals and fire stations, and ensure that public safety officials include information related to electrical safety and responses to long-duration power outages in their public briefings. (Recommendation 5.1)
- Utility regulators should work closely with operating utilities to assess their current interconnection standards as applicable to DERs, consider the costs of requiring new installations to use enhanced inverters, and determine the appropriate policy for promoting islanding and other related capabilities. (Recommendation 5.7)
- State legislatures and utility regulatory bodies should explore economic, ratemaking, and other regulatory options for facilitating the development of private microgrids that provide resilience benefits. (Recommendation 5.9)
- Utility regulators and non-governmental entities should undertake studies to develop guidance on how best to compensate the owners of distributed generation resources who are prepared to commit a portion of their distributed generation capacity to serve islanded feeders in the event of large outages of long duration. Additionally, the National Association of Regulatory Utility Commissioners (NARUC) should establish a working group to advise members on the issues they will likely have to address. (Recommendation 5.11)

**Recommendations Directed to the National Association of Regulatory Utility Commissioners and Federal Organizations**

NARUC is uniquely capable of convening and disseminating information to regulators from diverse states while providing a single point of contact with federal agencies.

**Recommendation 10 to NARUC and federal organizations:** The committee recommends that NARUC work with DHS and DOE as follows:

- Develop model guidance on how state regulators, utilities, and broader communities (where appropriate) might consider the equity and social implications of choices in the level and allocation of investments. (Recommendation 5.2)
- Develop guidance to state regulators and utilities on (1) selective restoration options as they become available,

(2) the factors that should be considered in making choices of which loads to serve, and (3) model recommendations that states and utilities can build upon and adapt to local circumstances. (Recommendation 5.4)

- Undertake studies of the technical, economic, and regulatory changes necessary to allow development and operation of privately owned microgrids that serve multiple parties and/or cross public rights-of-way. (Recommendation 5.8)

**Recommendation Directed to the Federal Energy Regulatory Commission and the North American Energy Standards Board**

The growing interdependence of natural gas and electricity infrastructures requires systematic study and targeted efforts to improve coordination and planning across the two industries.

**Recommendation 11 to FERC and the North American Energy Standards Board:** FERC, which has regulatory authority over both natural gas and electricity systems, should address the growing risk of interdependent infrastructure by doing the following:

- Working with the North American Energy Standards Board and industry stakeholders to improve awareness, communications, coordination, and planning between the natural gas and electric industries. (Recommendation 4.7)

**Recommendation Directed to the North American Electric Reliability Corporation**

Following large-scale outages, detailed investigations are essential to support the learning phase of resilience. NERC, with authority delegated from FERC, has conducted several such investigations.

**Recommendation 12 to NERC:** Review and improve incident investigation processes to better learn from outages that happen and broadly disseminate findings and best practices by doing the following:

- Engaging relevant regional and state-level organizations to improve the investigation process of large-scale losses of power, drawing lessons from the National Transportation Safety Board and others, with the objective of disseminating lessons across geographical and jurisdictional boundaries. (Recommendation 6.15)

**REFERENCES**

- Fischhoff, B., P. Slovic, and S. Lichtenstein. 1978. Fault trees: Sensitivity of estimated failure probabilities to problem representation. *Journal of Experimental Psychology: Human Perception and Performance* 4: 342–355.
- Kahneman, D. 2011. *Thinking Fast and Slow*. New York: Farrar, Straus, and Giroux.
- Kingdon, J.W. 1984. *Agendas, Alternatives, and Public Policies*. Boston: Little, Brown, and Company.
- Lindblom, C.E. 1959. The science of muddling through. *Public Administration Review* 19(2): 79–88.





# Appendix A

## Statement of Task

An ad hoc National Research Council (NRC) committee will address technical, policy and institutional factors that might affect how modern technology can be implemented in the evolution of electric transmission and distribution (T&D) in the United States, and recommend strategies and priorities for how the nation can move to a more reliable and resilient T&D system. The committee will consider how existing and emerging technological options, including greater reliance on distributed power generation, could impact the reliability, robustness, and the ability to recover from disruptions to the electrical T&D system or systems. The study will identify barriers to implementing technology pathways for improving T&D reliability, key priorities and opportunities including, where necessary, those for research, development and demonstration (RD&D), the federal role, and strategies and actions that could lead to a more reliable and resilient T&D system. As part of this study the committee may do the following:

1. Review recent studies and analysis of the current and projected status of the nation's electric T&D system including any that identify significant technological concerns over vulnerability, reliability, and resilience;
2. Assess factors affecting future requirements and trends for the nation's T&D infrastructure including such issues as the need for new capacity, replacement needs, siting issues, vulnerability to external threats and the need for security, whether physical or cyber, the alignment of costs and benefits, the effects of interconnectedness among regional networks, and others identified by the committee;
3. Evaluate the role existing and emerging technological options, especially of renewable and distributed generation technologies, can play in creating or addressing concerns identified by the committee and that can lead to enhanced reliability and resilience;
4. Consider how regional differences both in terms of the physical setting and the utility structure may impact solutions to improving resilience;
5. Review federal, state, industry, and academic R&D programs, as well as any demonstration and/or deployment efforts, focused on technologies for the T&D system that are aimed at improving its capacity, reliability, resilience, flexibility, and any other attributes aimed at enhancing the robustness of the nation's electric power T&D system;
6. Identify non-technological barriers (including those related to regulatory, ownership, and financial issues) to implementation of new and/or expanded technology to improve the stability, reliability, and resilience of electric T&D;
7. Suggest strategies, key opportunities and priorities, and actions for implementation of the identified technology pathways for the T&D system, which could include RD&D, policies, incentives, standards, and others the committee finds are necessary; and
8. Address the federal role, especially of DOE, in addressing the technical, policy, and institutional issues for a transformation of the T&D system to one with increased robustness and resilience.

# Appendix B

## Committee Biographies

M. GRANGER MORGAN, *Chair*, is Hamerschlag University Professor of Engineering; professor, Department of Engineering and Public Policy (where he served for 38 years as the founding department head) and Electrical and Computer Engineering at Carnegie Mellon University. He also holds an appointment in the H. John Heinz III College of Public Policy and Management. He is a fellow of the Institute of Electrical and Electronics Engineers (IEEE), the American Association for the Advancement of Science, and the Society for Risk Analysis. His research addresses problems in science, technology, and public policy with a particular focus on energy, environmental systems, climate change, and risk analysis. Much of his work has involved the development and demonstration of methods to characterize and treat uncertainty in quantitative policy analysis. At Carnegie Mellon, he co-directs (with Inês Azevedo) the Center for Climate and Energy Decision Making and (with Jay Apt) the Electricity Industry Center. He is a member of the National Academy of Sciences, serves on several committees for the National Academies of Sciences, Engineering, and Medicine, and is a member of several domestic and international advisory committees for organizations addressing issues involving electric power, other energy issues, and the management of risks to health safety and the environment. He holds a B.A. from Harvard College (1963) where he concentrated in physics, an M.S. in astronomy and space science from Cornell University (1965), and a Ph.D. from the Department of Applied Physics and Information Sciences at the University of California, San Diego (1969).

DIONYSIOS ALIPRANTIS is an associate professor of electrical and computer engineering at Purdue University. Dionysios obtained his Ph.D. from Purdue University in 2003 and his Diploma in electrical and computer engineering from the National Technical University of Athens, Greece, in 1999. Prior to joining Purdue, he was an assistant professor of electrical and computer engineering at Iowa State University. His research interests include electromagnetic energy conversion and electric machinery, power electronics, and

power systems analysis. More recently, his work has focused on technologies that enable the integration of renewable energy sources in the electric power system and the electrification of transportation. He is currently serving as an associate editor for the *IEEE Transactions on Energy Conversion*.

ANJAN BOSE is Regents Professor and Distinguished Professor of Electric Power Engineering at Washington State University. He has 50 years of experience in industry, academia, and government, as an engineer, educator, and administrator. He is also the site director of the National Science Foundation (NSF)-sponsored Power System Engineering Research Center. He served as the dean of the College of Engineering and Architecture (1998–2005) and as the director of the School of Electrical Engineering and Computer Science (1993–1998). Prior to Washington State University, he taught at Arizona State University (1981–1993) and worked in the Energy Management Systems Division of Control Data Corporation (now Siemens), where he developed power grid control software. He is a member of the U.S. National Academy of Engineering and the Indian National Academy of Engineering. A fellow of the IEEE, he was the recipient of the Outstanding Power Engineering Educator Award (1994), the Third Millennium Medal (2000), and the IEEE's Herman Halperin Electric Transmission and Distribution Award (2006). He has been recognized as a distinguished alumnus of the Indian Institute of Technology, Kharagpur (2005) and the College of Engineering at Iowa State University (1993). During 2011–2013, Bose served as senior advisor to the Department of Energy (DOE) coordinating priorities for the next-generation grid.

W. TERRY BOSTON is the former chief executive officer of PJM Interconnection, the largest power grid in North America and the largest electricity market in the world. Boston is past president of the Association of Edison Illuminating Companies and past president of GO 15, the association of the world's largest power grid operators. He also served as a U.S. vice president of the International Council of Large

Electric Systems and is a past chair of the North American Transmission Forum. He also was one of the eight industry experts selected to direct the North American Electric Reliability Corporation investigation of the August 2003 Northeast blackout. In 2011, Boston was honored with the Leadership in Power award from the IEEE Power and Energy Society. He also was chosen by *Intelligent Utilities* as one of the Top 11 Industry Movers and Shakers and led PJM to win Platts Global Energy Awards in Industry Leadership in 2010, Excellence in Electricity in 2012, and Lifetime Achievement Award in 2015. Boston is a member of the National Academy of Engineering. He received a B.S. in engineering from the Tennessee Technological University and an M.S. in engineering administration from the University of Tennessee.

ALLISON CLEMENTS is the president of goodgrid, LLC, based in Salt Lake City, Utah. She is the former director of the Sustainable Federal Energy Regulatory Commission (FERC) Project at Natural Resources Defense Council (NRDC). The Project represents a coalition of clean energy-focused advocacy organizations at FERC and at the independent system operator/regional transmission organization level in pursuit of a clean, reliable, and affordable electric system. Prior to joining the FERC Project, Clements spent 3 years as NRDC's corporate counsel while maintaining a policy practice in renewable energy deployment. Before joining NRDC, she worked as a project finance attorney at Chadbourne & Parke, LLP, as well as an energy regulatory attorney at Troutman Sanders, LLP. Clements is a 2015 Presidio Institute Cross-Sector Leadership Fellow, co-directed the Yale Law School and School of Forestry Environmental Protection Clinic (2013–2014), acted as co-chair of the Bipartisan Policy Center's Electric Grid Initiative (2011–2013), and served as a director and treasurer of the Healthy Building Network (2008–2014). She holds a B.S. in environmental policy from the University of Michigan and a J.D., with honors, from the George Washington University Law School.

JEFFERY DAGLE has been an electrical engineer at the Pacific Northwest National Laboratory since 1989. He currently manages several projects in the areas of transmission reliability and security, including the North American SynchroPhasor Initiative and cybersecurity reviews for the DOE Smart Grid Investment Grants and Smart Grid Demonstration Projects. He is a senior member of the IEEE and the National Society of Professional Engineers. He received the 2001 Tri-City Engineer of the Year award by the Washington Society of Professional Engineers, led the data requests and management task for the U.S.-Canada Power System Outage Task Force investigation of the August 14, 2003, blackout, supported the DOE Infrastructure Security and Energy Restoration Division with on-site assessments in New Orleans following Hurricane Katrina in fall 2005, and is the recipient of multiple patents including a Federal Laboratory Consortium Award in 2007 and an R&D 100 Award in 2008 for the

Grid Friendly™ Appliance Controller technology. Dagle was a member of a National Infrastructure Advisory Council study group formed in 2010 to establish critical infrastructure resilience goals. He received B.S. and M.S. degrees in electrical engineering from Washington State University in 1989 and 1994, respectively.

PAUL DE MARTINI is the managing director at Newport Consulting. He has more than 35 years of experience in the power industry. He is a thought leader and expert in the global electricity industry, providing guidance to utilities, policy makers, and new entrants. Previously, De Martini held several executive positions focused on strategy, policy, and technology development, including chief technology and strategy officer for Cisco's Energy Networks Business and vice president of Advanced Technology at Southern California Edison. De Martini has an M.B.A. from the University of Southern California and a B.S. in applied economics from the University of San Francisco. He is a visiting scholar at the California Institute of Technology.

JEANNE FOX is an adjunct professor at Columbia University's School of International and Public Affairs and at Rutgers University School of Arts and Sciences. She served as a commissioner of the New Jersey Board of Public Utilities from January 2002 until September 2014 and was its president and a member of the Governor's cabinet from January 2002 to January 2010. The New Jersey Board of Public Utilities has regulatory jurisdiction over telephone, electric, gas, water, wastewater, and cable television companies and works to ensure that consumers have proper service at reasonable rates. Commissioner Fox is currently a member of the National Petroleum Council and its Emergency Preparedness Committee, Carnegie Mellon University's Advisory Board for its Center for Climate Energy Decision Making, Rutgers University's Energy Institute Advisory Board, and GRID Alternatives Tri-State Board of Directors. Fox was active with the National Association of Regulatory Utility Commissioners as a member of the Board of Directors (2003–2014), Subcommittee on Education and Research, Subcommittee on Utility Market Access, Committee on Energy Resources and Environment (chair, vice chair), and Committee on Critical Infrastructure (vice chair). She is currently a member of the National Association of Regulatory Utility Commissioners' Emeritus. Fox served as Region 2 administrator of the United States Environmental Protection Agency (1994–2001) and as commissioner and deputy commissioner of the New Jersey Department of Environmental Protection and Energy (1991–1994). Starting at the Board of Public Utilities in 1981 as a regulatory officer, she was promoted to Solid Waste Division deputy director (1985), Water Division director (1987), and chief of staff (1990–1991). In 2001, Fox was a visiting distinguished lecturer at Rutgers University's Bloustein School of Planning and Public Policy and at Princeton University's Woodrow Wilson School of Public and International Affairs.

(2001–2002, 2016–2017). Fox is currently president of the associate alumnae of Douglass College and a Rutgers University trustee emerita. She is a member of the Rutgers Hall of Distinguished Alumni Award (1997) and the Douglass Society (1993) and a recipient of the Rutgers Alumni Federation Alumni Meritorious Service Award (1991) and the Loyal Sons and Daughters of Rutgers Award (2012). Fox graduated cum laude from Douglass College, Rutgers University, and received a J.D. from the Rutgers University School of Law, Camden.

ELSA GARMIRE is the former Sydney E. Junkins Professor at Thayer School of Engineering, Dartmouth College. She received her A.B. at Harvard and her Ph.D. at M.I.T., both in physics. After postdoctoral work at Caltech, she spent 20 years at the University of Southern California, where she was eventually named William Hogue Professor of Electrical Engineering and director of the Center for Laser Studies. She came to Dartmouth in 1995 as dean of Thayer School of Engineering. In her technical field of quantum electronics, lasers, and optics, she has authored more than 250 journal papers, obtained nine patents, and been on the editorial board of five technical journals. She has supervised 30 Ph.D. theses and 14 M.S. theses. Garmire is a member of the National Academy of Engineering, on whose Governing Council she has served, and the American Academy of Arts and Sciences. She is a fellow of IEEE, the American Physical Society, and the Optical Society of America, of which she was president in 1993. In 1994, she received the Society of Women Engineers Achievement Award. Garmire has been a Fulbright senior lecturer in fiber optics and a visiting faculty member in Japan, Australia, Germany, and China. She chaired the NSF Advisory Committee on Emerging Technology and served on both the NSF Advisory Committee on Engineering and the Air Force Science Advisory Board. With her electrical engineering background and fiber-optics expertise, she has followed the growing challenges to the nation's energy infrastructure, with particular interest in the electric grid.

RONALD E. KEYS, an independent consultant, retired from the Air Force in November 2007 after completing a career of more than 40 years. His last assignment was as Commander, Air Combat Command, the Air Force's largest major command, consisting of more than 1,200 aircraft, 27 wings, 17 bases, and 200 operating locations worldwide with 105,000 personnel. General Keys holds a B.S. from Kansas State University and an M.B.A. from Golden Gate University. General Keys is a command pilot with more than 4,000 flying hours in fighter aircraft, including more than 300 hours of combat time. No stranger to energy challenges, General Keys first faced them operationally as a young Air Force Captain, piloting F-4s during the fuel embargo of the 1970s. Later, as director of operations for European Command, fuel and logistic supply provisioning were critical

decisions during humanitarian, rescue, and combat operations across European Command's area of responsibility including the Balkans and deep into Africa. As Commander of Allied Air Forces Southern Europe and Commander of the U.S. 16th Air Force, similar hard choices had to be made in supporting OPERATION NORTHERN WATCH in Iraq as well as for combat air patrols and resupply in the Balkans. Later, as the director of all Air Force Air, Space, and Cyber mission areas as well as operational requirements in the early 2000s, he saw the impact of energy choices on budget planning and execution as well as in training and supporting operational plans in Iraq and Afghanistan. Finally, at Air Combat Command, he faced the total challenge of organizing, training, and equipping forces at home and deployed to balance mission effectiveness with crucial energy efficiency, security, and resilience. Continuing after retirement, he has advised the U.S. Air Force on energy security strategy planning and acted as a subject matter expert during analysis of energy impacts and trade-offs in "futures" war games. As a Bipartisan Center senior advisor, he served as a technical advisor on the "Cyber Shockwave" exercise based on cyber and physical grid and internet attacks. He is a member of The Center for Climate and Security's Advisory Board as well as their Climate and Security Working Group focused on developing policy options and encouraging dialogue and education. As chairman of the CNA Military Advisory Board on Department of Defense Energy Security and Climate Change, he is intimately familiar with the relationship of energy, military, economic, and national security and has contributed to a number of energy and climate reports, most recently concerning the vulnerability and resilience of the electric grid.

MARK McGRANAGHAN is vice president of distribution and energy utilization for the Electric Power Research Institute (EPRI). This research area is leading the development of the next generation integrated grid while continuing to develop new innovations for designing, maintaining, and improving the existing grid. This includes research to define and develop the information and communication infrastructure that will support the integrated grid. He has been involved in resiliency research at EPRI at both the transmission and distribution levels. McGranaghan has more than 35 years of experience in the industry. He has authored more than 70 technical papers and articles on topics ranging from power quality to insulation coordination of extra-high-voltage systems. He is an IEEE fellow and, in 2014, received the Charles Proteus Steinmetz award for his expertise and dedication to power engineering standards development. He has recently been one of the industry leaders developing the standards and platforms to support the next-generation smart grid for integration of widespread distributed resources. He is a member of the executive committee of the CIGRE U.S. National Committee, vice chairman of the CIRED U.S. National Committee, and a member



of the International Electrotechnical Commission Advisory Committee on Electricity Transmission and Distribution. McGranaghan has taught courses and seminars around the world to help support collaboration in the power industry. He is a co-author of the book *Electrical Power Systems Quality*, now in its third edition. McGranaghan has a B.S.E.E. from the University of Toledo and an M.B.A. from the University of Pittsburgh. In 2015, he received the Outstanding Alumni Award from the University of Toledo College of Engineering and Computer Science.

CRAIG MILLER currently serves full time as the National Rural Electric Cooperative Association's chief scientist. Miller is a technologist with extensive background in the physical sciences, information technology, and systems engineering. He has developed new technology and cutting-edge systems for more than 30 years, within and for both start-up and established corporations. His particular strength is the conceptualization, tuning, and positioning of new technology products. More than 2,000 companies in the United States use systems or technology he has architected or developed. Miller's many accomplishments deserve mention: participating in seven start-ups; serving as SAIC's chief scientist (during which time he was granted the "Heroic Achievement in Information Technology" award from the Smithsonian Institution); and a wide experience in technical and financial media as a key investor relations expert, technologist, inventor, and analyst on behalf of diverse companies such as Proxicom, GridPoint, DiData, and Aguru Images, a high-end digital imaging company that he started. More recently, Miller has achieved a national reputation in the advanced smart grid and cybersecurity arenas.

THOMAS J. OVERBYE is a Texas A&M Engineering Experiment Station Distinguished Research Professor in the Electrical and Computer Engineering Department at Texas A&M University. Formerly, he was the Fox Family Professor of Electrical and Computer Engineering at the University of Illinois, Urbana-Champaign, where he has taught since 1991. He received his B.S., M.S., and Ph.D. in electrical engineering from the University of Wisconsin, Madison and is a member of the National Academy of Engineering. His current research interests include electric power system analysis, visualization, dynamics, cybersecurity, and modeling of power system geomagnetic disturbances. Overbye is the original developer of the PowerWorld Simulator, an innovative computer program for power system analysis, education, and visualization; a co-founder of PowerWorld Corporation; and an author of *Power System Analysis and Design*. He was the recipient of the IEEE/Power and Energy Society Walter Fee Outstanding Young Engineer Award in 1993 and the IEEE/Power and Energy Society Outstanding Power Engineering Educator Award in 2011, and he participated in the 2003 DOE/North American Electric Reliability Corporation Blackout investigation.

WILLIAM H. SANDERS is Donald Biggar Willett Professor of Engineering and the head of the Department of Electrical and Computer Engineering at the University of Illinois, Urbana-Champaign. Dr. Sanders's research interests include secure and dependable computing and security and dependability metrics and evaluation, with a focus on critical infrastructures. He has published more than 270 technical papers in those areas. He served as the director and principal investigator of the DOE/Department of Homeland Security Trustworthy Cyber Infrastructure for the Power Grid Center, which is at the forefront of national efforts to make the U.S. power grid smart and resilient. He is also co-developer of three tools for assessing computer-based systems: METASAN, UltraSAN, and Möbius. Möbius and UltraSAN have been distributed widely to industry and academia; more than 1,700 licenses for the tools have been issued to universities, companies, and NASA for evaluating the performance, dependability, and security of a variety of systems. He is also a co-developer of the Network Access Policy Tool for assessing the security of networked systems; it is available commercially under the name NP-View from the start-up company Network Perception, which was cofounded by Dr. Sanders.

RICHARD E. SCHULER is a professor of economics (College of Arts and Sciences), a professor emeritus of civil and environmental engineering (College of Engineering), and a graduate school professor at Cornell University. Schuler served on the executive committee of the NSF-supported, multi-university Institute for Civil Infrastructure Systems. Previous administrative positions at Cornell have included director of the Waste Management Institute and the New York State Solid Waste Combustion Institutes (1987–1993), as associate director of the Center for the Environment (1989–1993), and director of Cornell's Institute for Public Affairs (1995–2001), a university-wide multidisciplinary program offering the M.P.A. degree. He has served on the Board of Trustees of Cornell University (1993–1997). Schuler's industrial and government experience include engineer and manager with the Pennsylvania Power and Light Company (1959–1968), energy economist with Battelle Memorial Institute (1968–1969), and public service commissioner and deputy chairman for New York State (1981–1983). He has been a consultant to numerous government agencies and industries on pricing, management, and environmental issues and to the World Bank on energy and infrastructure investment programs. From its inception in 1999 until April 2012, he was a founding board member of the New York Independent System Operator that is responsible for operating the electric transmission grid reliably in New York while overseeing an efficient power market. During his tenure he chaired the New York Independent System Operator board's market performance, reliability and markets, and its governance committees, and from 2008–2010 he was the board's lead director. Schuler's degrees include a B.E. in electrical

engineering, Yale, 1959; an M.B.A., Lehigh, 1969; and a Ph.D. in economics, Brown, 1972. He has been a registered professional engineer in Pennsylvania since 1963.

SUSAN TIERNEY is a senior advisor at Analysis Group and is an expert on energy economics, regulation, and policy, particularly in the electric and gas industries. She has consulted to businesses, governments, tribes, non-profit organizations, foundations, and other organizations on energy markets, economic and environmental regulation and strategy, and energy policy. She has participated as an expert in civil litigation cases, in regulatory proceedings before state and federal agencies, on a variety of boards and commissions, and on National Academies' committees. Previously, she served as the assistant secretary for policy at DOE. She was the secretary for environmental affairs in Massachusetts, commissioner at the Massachusetts Department of Public Utilities, chairman of the Board of the Massachusetts Water Resources Authority, and executive director of the Massachusetts Energy Facilities Siting Council. She chairs DOE's Electricity Advisory Committee as well as the External Advisory Board of the National Renewable Energy Laboratory, and she previously served on the Secretary of Energy Advisory Board. She is a director of the World Resources

Institute, Resources for the Future, and other boards. She has published widely, frequently speaks at industry conferences, and has lectured at many leading universities. Tierney received her Ph.D. and M.A. in regional planning from Cornell University.

DAVID G. VICTOR is director of the Laboratory on International Law and Regulation and a professor at the School of Global Policy and Strategy at the University of California, San Diego, where he also co-leads the university's Deep Decarbonization Initiative. His research focuses on how regulatory law affects the environment, technology choices, industrial structure, and the operation of major energy markets. Prior to joining the University of California, San Diego, Victor served as director of the Program on Energy and Sustainable Development at Stanford University where he was also a professor at the law school. He is a member of the Board of Directors of EPRI, on the advisory council for the Institute of Nuclear Power Plant Operators, and chairman of the Community Engagement Panel that is helping to guide the decommissioning of Units 2 and 3 at the San Onofre Nuclear Generating Station. He has contributed to numerous publications on topics such as energy market innovations and electric power market reform.

# Appendix C

## Disclosure of Conflicts of Interest

The conflict of interest policy of the National Academies of Sciences, Engineering, and Medicine ([www.nationalacademies.org/coi](http://www.nationalacademies.org/coi)) prohibits the appointment of an individual to a committee like the one that authored this Consensus Study Report if the individual has a conflict of interest that is relevant to the task to be performed. An exception to this prohibition is permitted only if the National Academies determine that the conflict is unavoidable and the conflict is promptly and publicly disclosed.

When the committee that authored this report was established, a determination of whether there was a conflict of interest was made for each committee member given the individual's circumstances and the task being undertaken by the committee. A determination that an individual has a conflict of interest is not an assessment of that individual's actual behavior, character, or ability to act objectively despite the conflicting interest.

Mr. Paul De Martini was determined to have a conflict of interest because he is the managing director at Newport Consulting. Dr. Susan Tierney was determined to have a conflict of interest because she is the senior advisor at Analysis Group and also performs consulting work.

In each case, the National Academies determined that the experience and expertise of the individual was needed for the committee to accomplish the task for which it was established. The National Academies could not find another available individual with the equivalent experience and expertise who did not have a conflict of interest. Therefore, the National Academies concluded that the conflict was unavoidable and publicly disclosed it through the National Academies' Current Projects System ([www8.nationalacademies.org/cp](http://www8.nationalacademies.org/cp)).

# Appendix D

## Presentations and Committee Meetings

### FIRST COMMITTEE MEETING MARCH 2–3, 2016 WASHINGTON, D.C.

FERC Activities in the Office of Electric Reliability  
*Michael Bardee, Federal Energy Regulatory Commission, Office of Electric Reliability*

EPRI Activities in Electricity Sector Modernization  
*Mark McGranaghan, Electric Power Research Institute*

NERC and APPA Activities in Critical Infrastructure Protection  
*Nathan Mitchell, American Public Power Association*

DOE Office of Electricity Perspective on NAS Committee Task  
*Patricia Hoffman, Department of Energy, Office of Electricity Delivery and Energy Reliability*

### SECOND COMMITTEE MEETING MAY 11–12, 2016 WASHINGTON, D.C.

Overview of Relevant DOE Activities and Needs  
*Gilbert Bindewald, Department of Energy, Office of Electricity Delivery and Energy Reliability*

Improving Resilience of Transformers  
*Richard Boyd, Siemens*  
*James McIver, Siemens*

Resilience Through Relays, Sensors, and Components  
*Gregory Zweigle, Schweitzer Engineering Laboratories*

Resilience through Automation and Trade-offs with Cybersecurity  
*Steven Kunsman, ABB*

Cybersecurity and Activities in NERC and E-ISAC  
*Tim Roxey, Electricity Information Sharing and Analysis Center*

### THIRD COMMITTEE MEETING JULY 11–12, 2016 WASHINGTON, D.C.

Panel on State Regulatory Commissions and Resilience  
*Paul Centolella, Paul Centolella and Associates*  
*David Littell, Regulatory Assistance Project*  
*Kris Mayes, Utility of the Future Center*  
*Audrey Zibelman, New York State Public Service Commission*

Extreme Weather Events  
*Tom Karl, National Oceanic and Atmospheric Administration's National Centers for Environmental Information*  
*Jim Kossin, National Oceanic and Atmospheric Administration's National Centers for Environmental Information*  
*Ken Kunkel, National Oceanic and Atmospheric Administration's National Centers for Environmental Information*  
*Mike Squires, National Oceanic and Atmospheric Administration's National Centers for Environmental Information*

Trends in Battery Storage  
*Jay Whitacre, Carnegie Mellon University*

### FOURTH COMMITTEE MEETING SEPTEMBER 29–30, 2016 WASHINGTON, D.C.

Utility Perspectives on Resilience  
*Joe Svachula, Commonwealth Edison*  
*Ralph LaRossa, Public Service Enterprise Group*  
*William Ball, Southern Company*  
*Erik Takayesu, Southern California Edison*

Distribution Resilience with High Automation  
*Jim Glass, Chattanooga Electric Power Board*

*APPENDIX D*

151

Briefing on RAND Resilience Report  
*Henry Willis, RAND Corporation*  
Industry-wide Trends in Resilience  
*David Owens, Edison Electric Institute*

**FIFTH COMMITTEE MEETING  
NOVEMBER 2–3, 2016  
WASHINGTON, D.C.**

No open session presentations were held at this meeting.

**SIXTH COMMITTEE MEETING  
FEBRUARY 15–16, 2017  
WASHINGTON, D.C.**

No open session presentations were held at this meeting.



# Appendix E

## Examples of Large Outages

### **NORTHEAST BLACKOUT AFFECTING UNITED STATES AND SOUTHEAST CANADA (AUGUST 13, 2003)**

#### **Pre-Event**

Due to the minimal amount of warning time before this event, no significant preparations were taken.

#### **Event**

High electricity demand in central Ohio combined with scheduled maintenance of several generators resulted in low voltage around the Cleveland-Akron area. Computer and alarm systems failed to warn operators due to software bugs in both the power company's and regulating authority's computer systems. Three 345 kV lines feeding central Ohio tripped due to contact with trees. Cascading failures resulted throughout the region as lower-voltage lines attempted and failed to take on the redistributed load from tripped lines. The blackout affected at least 50,000,000 customers, caused a loss of 70,000 MW, cost \$4–10 billion, and contributed to 11 deaths.

#### **Recovery**

Most areas were restored to full power within hours, but some areas in the United States were without power for 4 days. Parts of Ontario experienced rotating blackouts for up to 2 weeks. Physical damage was limited, making recovery much faster than other types of events.

#### **Lessons Learned**

Improvements in system protection to slow or limit cascading failures should be made. Improvements in operator training, emergency response plans, communication between reliability coordinators and utilities, and sensor usage should

also be made. Managing and pruning of vegetation and vegetation-caused bulk incidents should be reported to the North American Electric Reliability Corporation (NERC) and regional reliability coordinators (NERC, 2004).

### **WEST COAST BLACKOUT (AUGUST 10, 1996)**

#### **Pre-Event**

Due to the minimal amount of warning time before this event, no significant preparations were taken.

#### **Event**

Heavy loading on 500 kV transmission lines and the western interconnect system was caused by good hydro conditions in the northwest region and high demand in California resulting from high summer temperatures. The 500 kV Big Eddy-Ostrander line arced to a tree, followed by four more 500 kV lines over 100 minutes. Several smaller lines also arced and closed. Systems protections removed 1,180 MW of generation from the system, creating an unstable power oscillation and ultimately causing islanding of the Western Electricity Coordinating Council into four distinct islands: Island 1, Alberta, Canada; Island 2, Colorado to British Columbia; Island 3, Central to Northern California; and Island 4, Southern California to New Mexico to Northern Mexico. The outage affected approximately 7,500,000 customers and caused a loss of 33,024 MW.

#### **Recovery**

Physical damage was limited, making recovery much faster than other types of events. Islands 1 and 2 had power restored within 2 hours. Island 3 was restored within 9 hours. Island 4 was restored within 6 hours.

## APPENDIX E

**Lessons Learned**

Limiting certain high-voltage lines would prevent cascading failures. Insuring coordination between power producers and transmission operators is imperative (NERC, 2002).

**GEOMAGNETIC DISTURBANCE AFFECTING EASTERN CANADA (MARCH 13, 1989)****Pre-Event**

Due to the small amount of warning time before this event, no significant preparations were taken. However, forecasts for solar storm events may enable preparation in the future.

**Event**

At 2:45 a.m., a solar magnetic storm resulting from a solar flare tripped five lines in Eastern Canada by inducing a quasi-direct current. The land surrounding the Hudson Bay rests on an igneous rock shield, making the region more susceptible to ground-induced currents that result from solar storms. Higher latitudes also determine a location's magnetic storm vulnerability. The outage affected approximately 6,000,000 customers and caused a loss of 19,400 MW.

**Recovery**

Forty-eight percent of power was restored after 5 hours. Eighty-three percent of power was restored after 9 hours. Some strategic equipment and two major step-up transformers were damaged and required repair due to overvoltage.

**Lessons Learned**

NERC urged the National Oceanic and Atmospheric Administration for the capabilities and coordination for at least 1 hour of notice of solar storms. Forecasting remains less precise compared to meteorological events but still has potential to give minutes to hours of warning to grid operators for the approach of strong solar storms. Current standards require systems to withstand benchmark geomagnetic disturbance events, particularly to prevent high-voltage transformers from overheating (NERC, 1989).

**ICE STORM AFFECTING SOUTHERN CANADA AND THE NORTHEAST UNITED STATES (JANUARY 10, 1998)****Pre-Event**

The severity of the ice storm was poorly predicted since icing conditions depend critically on the vertical atmospheric temperature profile. As a result, officials did not make any significant preparations for this event.

**Event**

During a series of severe ice storms beginning on January 5, heavy ice and snow loads caused the destruction of trees and high-voltage towers. Thirty thousand wooden utility poles collapsed, leaving millions without power. Two major generating stations were disconnected from the rest of the grid due to line tripping, causing the area to blackout. The bulk transmission grid remained mostly intact, keeping the outage from spreading too far outside of the Québec area. The outage affected 2,800,000 customers and caused a loss of 18,500 MW.

**Recovery**

Hundreds of utility crews from outside the area were brought in, along with 16,000 Canadian military personnel, making this the largest deployment of Canadian military since the Korean War. American military also assisted in recovery efforts. Northern New York and New England had their power returned within 3 weeks. Québec had its power back online within 4 weeks.

**Lessons Learned**

Disruptions of telephone, cellular, and fiber-optic cables made communication difficult. The most reliable means of communications were found to be the utility-owned and operated microwave and mobile radio systems. More accurate temperature profiling and precautions around temperatures where ice storms are possible would be beneficial for preparing for any outage that results from these types of storms. Building towers and lines to withstand greater weights from icing would also result in greater resilience (NERC, 2001).

**HURRICANE SANDY AFFECTING THE NORTHEAST UNITED STATES (OCTOBER 29, 2012)****Pre-Event**

Unlike unexpected cascading failures or solar storms, hurricanes typically offer days of warning before outages occur. In the days leading up to landfall, extensive communication was made between utilities and generating facilities to prepare for abnormal operation, including preparing black-start units with enough fuel for emergency use. Additional field operation crews were made available for response. Sandbags and other barriers were put around vulnerable substations. In the minutes and hours leading up to outages, flood-prone areas were de-energized.

**Event**

Superstorm Sandy made landfall over New Jersey, New York, and the northern mid-Atlantic with wind speeds of

about 80 mph at landfall and a storm surge that flooded low-lying assets, causing more than 260 transmission trips and loss of roughly 20,000 MW of generation capacity. High winds and flooding were the major causes of outages, with some snow and icing contributing as well. More than 5,770,000 customers were affected.

### Recovery

Ninety-five percent of customers' power was restored between November 1, 2012, and November 9, 2012.

### Lessons Learned

Pre-staging equipment for recovery and de-energizing facilities in flood-prone areas can mitigate losses and hasten recovery. Implementing flood-protected facilities that include water-tight doors and barricades would prevent some stations from tripping (NERC, 2014).

### REFERENCES

- NERC (North American Electric Reliability Corporation). 1989. *March 13, 1989 Geomagnetic Disturbance*. <http://www.nerc.com/files/1989-Quebec-Disturbance.pdf>.
- NERC. 2001. *1998 System Disturbances: Review of Selected Electric System Disturbances in North America*. <http://www.nerc.com/pa/rrm/ea/System%20Disturbance%20Reports%20DL/1998SystemDisturbance.pdf>.
- NERC. 2002. *Review of Selected 1996 Electric System Disturbances in North America*. <http://www.nerc.com/pa/rrm/ea/System%20Disturbance%20Reports%20DL/1996SystemDisturbance.pdf>.
- NERC. 2004. *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* [http://www.nerc.com/docs/blackout/NERC\\_Final\\_Blackout\\_Report\\_07\\_13\\_04.pdf](http://www.nerc.com/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf).
- NERC. 2014. *Hurricane Sandy Event Analysis Report*. [http://www.nerc.com/pa/rrm/ea/Oct2012HurricaneSandyEventAnalysisReportDL/Hurricane\\_Sandy\\_EAR\\_20140312\\_Final.pdf](http://www.nerc.com/pa/rrm/ea/Oct2012HurricaneSandyEventAnalysisReportDL/Hurricane_Sandy_EAR_20140312_Final.pdf).

# Appendix F

## Acronyms

AC	alternating current
AMI	advanced metering infrastructure
APS	Arizona Public Services
BPA	Bonneville Power Administration
C&I	commercial and industrial
CAISO	California Independent System Operator
CAP	Civil Air Patrol
CHP	combined heat and power
CIP	critical infrastructure protection
DC	direct current
DER	distributed energy resource
DES	distributed energy storage
DG	distributed generation
DHS	Department of Homeland Security
DMS	distribution management system
DOD	Department of Defense
DOE	Department of Energy
DR	demand response
DSO	distribution system operator
E-ISAC	Electricity Information Sharing and Analysis Center
EEI	Edison Electric Institute
EIA	Energy Information Administration
EIM	Energy Imbalance Market
EMP	electromagnetic pulse
EMS	energy management system
EPAct	Energy Policy Act
EPB	Electric Power Board
EPRI	Electric Power Research Institute
ERCOT	Electric Reliability Council of Texas
ERD	entity relationship diagram
FAA	Federal Aviation Administration
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FPA	Federal Power Act

GMD	geomagnetic disturbance
GMLC	Grid Modernization Laboratory Consortium
GPS	global positioning satellites
GW	gigawatt
ICC	Illinois Commerce Commission
ICS	industrial control system
IEEE	Institute of Electrical and Electronics Engineers
IPCC	Intergovernmental Panel on Climate Change
ISO	independent system operator
JCESR	Joint Center for Energy Storage Research
LOLP	loss of load probability
LPT	large power transformer
MAA	mutual assistance agreement
MW	megawatt
NARUC	National Association of Regulatory Utility Commissioners
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NPS	National Preparedness System
NRC	National Research Council
NRCC	National Response Coordination Center
NRDC	National Resources Defense Council
NSF	National Science Foundation
OMS	outage management system
OT	operational technology
PMU	phasor measurement unit
PSEG	Public Service Enterprise Group
PUC	public utility commission
PURPA	Public Utility Regulation Policy Act
PV	photovoltaic
QER	Quadrennial Energy Review
R&D	research and development
RD&D	research, demonstration, and development
RTO	regional transmission organization
RTU	remote terminal unit
RUS	Rural Utility Service
SAIDI	system average interruption duration index
SAIFI	system average interruption frequency index
SCADA	supervisory control and data acquisition
SoCo	Southern Company
T&D	transmission and distribution
UAV	unmanned aerial vehicle